

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masanao SAKAI
Title: NETWORK, IPsec SETTING SERVER APPARATUS, IPsec
PROCESSING APPARATUS, AND IPsec SETTING METHOD USED
THEREFOR
Appl. No.: Unassigned
Filing Date: 09/05/2003
Examiner: Unassigned
Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2002-264913
filed 09/11/2002.

Respectfully submitted,

Michael M. A. Blumenthal
Reg No. 34,717

By _____

for

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Date: September 5, 2003

FOLEY & LARDNER
Customer Number: 22428



22428

PATENT TRADEMARK OFFICE

Telephone: (202) 672-5407
Facsimile: (202) 672-5399

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年 9月11日
Date of Application:

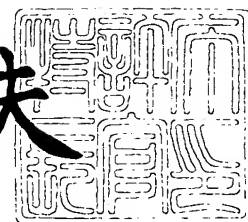
出願番号 特願2002-264913
Application Number:
[ST. 10/C]: [JP 2002-264913]

出願人 日本電気株式会社
Applicant(s):

2003年 8月12日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3064761

【書類名】 特許願

【整理番号】 41810227

【提出日】 平成14年 9月11日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 酒井 征直

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100088812

【弁理士】

【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

【予納台帳番号】 030982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク、IPsec 設定サーバ装置、IPsec 処理装置及びそれらに用いる IPsec 設定方法

【特許請求の範囲】

【請求項 1】 異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置と、前記 IPsec 処理装置の IPsec 設定を管理する IPsec 設定サーバ装置とを含むネットワークであって、第 1 及び第 2 の IPsec 処理装置間に適用する前記 IPsec のポリシーを一括管理する機能を前記 IPsec 設定サーバ装置に有することを特徴とするネットワーク。

【請求項 2】 前記第 1 の IPsec 処理装置から受信した前記第 2 の IPsec 処理装置との間の通信に対する要求メッセージの内容を基に前記第 2 の IPsec 処理装置との間に適用する前記 IPsec のポリシーを特定する機能を前記 IPsec 設定サーバ装置に含むことを特徴とする請求項 1 記載のネットワーク。

【請求項 3】 前記要求メッセージを受信した場合に当該要求メッセージを送信した前記第 1 の IPsec 処理装置の通信相手である前記第 2 の IPsec 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記 IPsec 設定サーバ装置に含むことを特徴とする請求項 2 記載のネットワーク。

【請求項 4】 前記要求起動メッセージに対する応答がない時に前記第 1 の IPsec 処理装置に対して前記第 2 の IPsec 処理装置からの応答なしを通知する機能を前記 IPsec 設定サーバ装置に含むことを特徴とする請求項 3 記載のネットワーク。

【請求項 5】 前記要求メッセージの内容とそれに適用する前記 IPsec のポリシーの内容とから当該 IPsec 通信に必要となる SA (Security Association) パラメータを生成する機能を前記 IPsec 設定

サーバ装置に含むことを特徴とする請求項 2 から請求項 4 のいずれか記載のネットワーク。

【請求項 6】 前記要求メッセージに対して前記 IPsec のポリシーと前記 SA パラメータとを少なくとも含む配布メッセージを送信する機能を前記 IPsec 設定サーバ装置に含むことを特徴とする請求項 2 から請求項 5 のいずれか記載のネットワーク。

【請求項 7】 前記 IPsec の暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 IPsec 処理装置に配布する機能とを前記 IPsec 設定サーバ装置に含むことを特徴とする請求項 1 から請求項 6 のいずれか記載のネットワーク。

【請求項 8】 異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置の IPsec 設定を管理する IPsec 設定サーバ装置であって、前記 IPsec 処理装置間に適用する前記 IPsec のポリシーを一括管理する機能を有することを特徴とする IPsec 設定サーバ装置。

【請求項 9】 前記 IPsec 処理装置から受信した他の IPsec 処理装置との間の通信に対する要求メッセージの内容を基に前記他の IPsec 処理装置との間に適用する前記 IPsec のポリシーを特定する機能を含むことを特徴とする請求項 8 記載の IPsec 設定サーバ装置。

【請求項 10】 前記要求メッセージを受信した場合に当該要求メッセージを送信した IPsec 処理装置の通信相手の IPsec 処理装置に対して当該通信の要求メッセージを送信させるために要求起動メッセージを送信する機能を含むことを特徴とする請求項 9 記載の IPsec 設定サーバ装置。

【請求項 11】 前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信した IPsec 処理装置に対して前記通信相手の IPsec 処理装置からの応答なしを通知する機能を含むことを特徴とする請求項 10 記載の前記 IPsec 設定サーバ装置。

【請求項 12】 前記要求メッセージの内容とそれに適用する前記 IPsec

c のポリシーの内容とから当該 IPsec 通信に必要となる SA (Security Association) パラメータを生成する機能を含むことを特徴とする請求項 9 から請求項 11 のいずれか記載の IPsec 設定サーバ装置。

【請求項 13】 前記要求メッセージに対して前記 IPsec のポリシーと前記 SA パラメータとを少なくとも含む配布メッセージを送信する機能を含むことを特徴とする請求項 9 から請求項 12 のいずれか記載の IPsec 設定サーバ装置。

【請求項 14】 前記 IPsec の暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 IPsec 処理装置に配布する機能とを含むことを特徴とする請求項 8 から請求項 13 のいずれか記載の IPsec 設定サーバ装置。

【請求項 15】 インタネットにおいて IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置であって、前記 IPsec を適用すべきパケットを受信した場合に IPsec 設定サーバ装置で一括管理される当該 IPsec に関する設定を前記 IPsec 設定サーバ装置に問い合わせるか否かを判断する機能を有することを特徴とする IPsec 処理装置。

【請求項 16】 前記 IPsec に関する設定を取得するために前記 IPsec 設定サーバ装置に他の IPsec 処理装置との間の通信に対する要求メッセージを送信する機能を含むことを特徴とする請求項 15 記載の IPsec 処理装置。

【請求項 17】 前記 IPsec 設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行うことを特徴とする請求項 16 記載の IPsec 処理装置。

【請求項 18】 前記 IPsec 設定サーバ装置から受信した配布メッセージを基に前記 IPsec を適用するためのポリシーを記録する SPD 及び個々の通信に対して前記 IPsec の処理を実施するために必要な SA (Security Association) を記録する SAD を設定する機能を含むことを特徴とする請求項 15 から請求項 17 のいずれか記載の IPsec 処理装置。

【請求項 1 9】 前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を前記 I P s e c 設定サーバ装置から取得する機能を含むことを特徴とする請求項 1 5 から請求項 1 8 のいずれか記載の I P s e c 処理装置。

【請求項 2 0】 前記 S A の有効期限が満了する前に前記 I P s e c 設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得する機能を含むことを特徴とする請求項 1 5 から請求項 1 9 のいずれか記載の I P s e c 処理装置。

【請求項 2 1】 異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) を使用する I P s e c 処理装置と、前記 I P s e c 処理装置の I P s e c 設定を管理する I P s e c 設定サーバ装置とからなるネットワークの I P s e c 設定方法であって、前記 I P s e c 処理装置間に適用する前記 I P s e c のポリシーを一括管理するステップを前記 I P s e c 設定サーバ装置に有することを特徴とする I P s e c 設定方法。

【請求項 2 2】 前記 I P s e c 処理装置から受信した他の I P s e c 処理装置との間の通信に対する要求メッセージの内容を基に前記他の I P s e c 処理装置との間に適用する前記 I P s e c のポリシーを特定するステップを前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 2 1 記載の I P s e c 設定方法。

【請求項 2 3】 前記要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 処理装置の通信相手の I P s e c 処理装置に対して当該通信の要求メッセージを送信させるために要求起動メッセージを送信するステップを前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 2 2 記載の I P s e c 設定方法。

【請求項 2 4】 前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信した I P s e c 処理装置に対して前記通信相手の I P s e c 処理装置からの応答なしを通知する機能を前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 2 3 記載の I P s e c 設定方法。

【請求項 25】 前記要求メッセージの内容とそれに適用する前記 I P s e c のポリシーの内容とから当該 I P s e c 通信に必要となる S A (S e c u r i t y A s s o c i a t i o n) パラメータを生成するステップを前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 22 または請求項 24 記載の I P s e c 設定方法。

【請求項 26】 前記要求メッセージに対して前記 I P s e c のポリシーと前記 S A パラメータとを少なくとも含む配布メッセージを送信するステップを前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 22 から請求項 25 のいずれか記載の I P s e c 設定方法。

【請求項 27】 前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記 I P s e c 処理装置に配布するステップとを前記 I P s e c 設定サーバ装置に含むことを特徴とする請求項 21 から請求項 26 のいずれか記載の I P s e c 設定方法。

【請求項 28】 前記 I P s e c 処理装置が、前記 I P s e c を適用すべきパケットを受信した場合に I P s e c 設定サーバ装置で一括管理される当該 I P s e c に関する設定を前記 I P s e c 設定サーバ装置に問い合わせるか否かを判断することを特徴とする請求項 21 から請求項 27 のいずれか記載の I P s e c 設定方法。

【請求項 29】 前記 I P s e c 処理装置が、前記 I P s e c に関する設定を取得するために前記 I P s e c 設定サーバ装置に他の I P s e c 処理装置との間の通信に対する要求メッセージを送信することを特徴とする請求項 21 から請求項 28 のいずれか記載の I P s e c 設定方法。

【請求項 30】 前記 I P s e c 処理装置が、前記 I P s e c 設定サーバ装置から受信した配布メッセージを基に前記 I P s e c を適用するためのポリシーを記録する S P D 及び個々の通信に対して前記 I P s e c の処理を実施するために必要な S A (S e c u r i t y A s s o c i a t i o n) を記録する S A D を設定することを特徴とする請求項 21 から請求項 29 のいずれか記載の I P s e c 設定方法。

【請求項 31】 前記 I P s e c 処理装置が、前記 I P s e c の暗号化や認

証に使用するための共有秘密鍵を前記 I P s e c 設定サーバ装置から取得することを特徴とする請求項 2 1 から請求項 3 0 のいずれか記載の I P s e c 設定方法。

【請求項 3 2】 前記 I P s e c 処理装置が、前記 S A の有効期限が満了する前に前記 I P s e c 設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得することを特徴とする請求項 2 1 から請求項 3 1 のいずれか記載の I P s e c 設定方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はネットワーク、I P s e c 設定サーバ装置、I P s e c 処理装置及びそれらに用いる I P s e c 設定方法に関し、特にインターネット上で機密性、完全性、認証等の機能を提供する I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) によるネットワーク構成に関する。

【 0 0 0 2 】

【従来の技術】

従来、インターネットの普及に伴って、インターネット上でのセキュリティを確保したいという要望が高まっている。特に、多くの企業においては、高価な専用線を用いてネットワークを構築する代わりに、インターネット上に仮想的な私設網を構築し、遠隔地のオフィス等を結ぶネットワークを安価に構築したいという要望も多い。

【 0 0 0 3 】

このような要望に対して、インターネット上で機密性、完全性、認証等の機能を提供する I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) が I E T F (I n t e r n e t E n g i n e e r i n g T a s k F o r c e) によって標準化されている（例えば、特許文献 1 参照）。

【 0 0 0 4 】

I P s e c を用いることによって、異なる 2 つの拠点間をインターネットを介し

て通信する場合には、インターネット経路上でのセキュリティを確保することが可能となる。新しいインターネットプロトコルである IPv6 (Internet Protocol version 6) では IPsec のサポートが必須となり、今後、ますます多くのネットワーク機器が IPsec に対応し、IPsec を使用した通信もますます増えることが予想される。

【0005】

この IPsec を使用した通信を行う IPsec 処理装置の構成を図 31 に示す。図 31 において、IPsec 処理装置 4 はインタフェース部 (I/F) 41, 42 と、IPsec 処理部 43 と、SPD (Security Policy Database) 44 と、SAD (Security Association Database) 45 と、ルーティング部 46 とを具備している。

【0006】

インタフェース部 41 はプライベートネットワークに接続され、プライベートネットワークとのデータ通信を行う。インタフェース部 42 はインターネットに接続され、インターネットを介したデータ通信を行う。

【0007】

IPsec 処理部 43 はインタフェース部 41, 42 から受信したデータ通信パケットに対して IPsec 処理を実施する。SPD 44 は IPsec 処理部 43 から参照され、IPsec を適用するためのポリシーが記録されている。SAD 45 は IPsec 処理部 43 から参照され、個々の通信に対して IPsec 処理を実施するために必要な SA が記録されている。ルーティング部 46 は IPsec 処理部 43 との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【0008】

特開 2001-298449 号公報 (第 8-11 頁、図 1)

【0009】

【発明が解決しようとする課題】

しかしながら、上述した従来の IPsec によるネットワーク構成では、1 台の IPsec 処理装置が多くの相手と IPsec 通信を実施する場合、IPse

cによる接続において、IPsec処理を実施する装置に設定する内容が多いという問題がある。

【0010】

IPsecを利用するためには、IPsecを適用する通信に対して使用するサービス[AH (Authentication Header: 認証ヘッダ)、ESP (Encapsulating Security Payload: カプセル化セキュリティペイロード) によって提供されるサービス]、使用するアルゴリズム等を、IPsec処理を実施する両端の装置にそれぞれ設定する必要がある。

【0011】

自動鍵管理プロトコル(IKE: Internet Key Exchange)を使用する場合には、自動鍵管理プロトコルで利用される暗号化アルゴリズム、ハッシュアルゴリズム、鍵共有アルゴリズム等も両端の装置に設定する必要がある。これらの設定の数はIPsecによって接続する相手毎に必要となるため、IPsecによって接続する相手が多くなるほど、多くの設定が必要となる。

【0012】

また、従来のIPsecによるネットワーク構成では、IPsecを適用する通信の両端で異なる設定をしてしまう可能性があるという問題がある。IPsec処理を実施する両端の装置において、使用するサービスの設定や、使用するアルゴリズムの設定に異なる設定をしてしまった場合、通信することができなくなる。IPsecを適用する通信が多くなると、設定の数も多くなるため、このような間違いが発生する可能性も増える。

【0013】

さらに、従来のIPsecによるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、共有秘密鍵を生成する演算に時間がかかり、結果として通信を開始することができるまでに時間がかかるとという問題がある。通常、IPsec処理装置では、図32に示すように、当該通信が必要になった時点で初めて共有秘密鍵の生成を始めるため、共有秘密鍵の生成に時間がかかれば、通信開

始までに時間がかかってしまう。

【0014】

さらにまた、従来の IPsec によるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、IPsec 処理を実施する装置に演算負荷が発生するという問題がある。共有秘密鍵を生成するためには多くの演算が必要となり、当該装置の持つ他の機能（IPsec を適用しないパケットの転送機能等）の性能が低下してしまう。同時に扱う IPsec 通信が多くなると、共有秘密鍵を生成する機会も多くなり、性能が低下する割合も多くなる。

【0015】

そこで、本発明の目的は上記の問題点を解消し、通信する装置間での設定不一致を防止することができるネットワーク、IPsec 設定サーバ装置、IPsec 処理装置及びそれらに用いる IPsec 設定方法を提供することにある。

【0016】

また、本発明の他の目的は、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるネットワーク、IPsec 設定サーバ装置、IPsec 処理装置及びそれらに用いる IPsec 設定方法を提供することにある。

【0017】

また、本発明の別の目的は、秘密鍵演算を不要とし、個々の装置での通信開始時の IPsec 経路の接続時間を短縮することができ、性能の低下を防ぐことができるネットワーク、IPsec 設定サーバ装置、IPsec 処理装置及びそれらに用いる IPsec 設定方法を提供することにある。

【0018】

【課題を解決するための手段】

本発明によるネットワークは、異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置と、前記 IPsec 処理装置の IPsec 設定を管理する IPsec 設定サーバ装置とを含むネットワークであって、前記 IP

s e c 処理装置間に適用する前記 I P s e c のポリシーを一括管理する機能を前記 I P s e c 設定サーバ装置に備えている。

【 0 0 1 9 】

本発明による他のネットワークは、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 処理装置の通信相手の I P s e c 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記 I P s e c 設定サーバ装置に具備している。

【 0 0 2 0 】

本発明による別のネットワークは、上記の構成のほかに、前記 I P s e c の暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 I P s e c 処理装置に配布する機能とを前記 I P s e c 設定サーバ装置に具備している。

【 0 0 2 1 】

本発明による I P s e c 設定サーバ装置は、異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) を使用する I P s e c 処理装置の I P s e c 設定を管理する I P s e c 設定サーバ装置であって、前記 I P s e c 処理装置間に適用する前記 I P s e c のポリシーを一括管理する機能を備えている。

【 0 0 2 2 】

本発明による他の I P s e c 設定サーバ装置は、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 処理装置の通信相手の I P s e c 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を具備している。

【 0 0 2 3 】

本発明による別の I P s e c 設定サーバ装置は、上記の構成のほかに、前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記 I P s e c 処理装置に配布する機能とを具備してい

る。

【0024】

本発明による IPsec 処理装置は、インターネットにおいて IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置であって、前記 IPsec を適用すべきパケットを受信した場合に IPsec 設定サーバ装置で一括管理される当該 IPsec に関する設定を前記 IPsec 設定サーバ装置に問い合わせるか否かを判断する機能を備えている。

【0025】

本発明による他の IPsec 処理装置は、上記の構成において、前記 IPsec 設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行っている。

【0026】

本発明による別の IPsec 処理装置は、上記の構成のほかに、前記 IPsec の暗号化や認証に使用するための共有秘密鍵を前記 IPsec 設定サーバ装置から取得する機能を具備している。

【0027】

本発明による IPsec 設定方法は、異なる 2 つの拠点間をインターネットを介して通信する場合にインターネット経路上でのセキュリティを確保するための IPsec (Internet Protocol security protocol) を使用する IPsec 処理装置と、前記 IPsec 処理装置の IPsec 設定を管理する IPsec 設定サーバ装置とからなるネットワークの IPsec 設定方法であって、前記 IPsec 処理装置間に適用する前記 IPsec のポリシーを一括管理するステップを前記 IPsec 設定サーバ装置に備えている。

【0028】

本発明による他の IPsec 設定方法は、上記の動作において、前記要求メッセージを受信した場合に当該要求メッセージを送信した IPsec 処理装置の通信相手の IPsec 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信するステップを前記 IPsec 設定サーバ装置

に具備している。

【0029】

本発明による別の I P s e c 設定方法は、上記のステップのほかに、前記 I P s e c の暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記 I P s e c 処理装置に配布するステップとを前記 I P s e c 設定サーバ装置に具備している。

【0030】

すなわち、本発明の I P s e c 設定方法は、インターネットにおいて I P s e c (I n t e r n e t P r o t o c o l s e c u r i t y p r o t o c o l) を使用する I P s e c 処理装置において、個々の I P s e c 処理装置に設定するポリシーを I P s e c 設定サーバに一括して登録することによって、個々の I P s e c 処理装置に設定するポリシーの数を削減するものである。

【0031】

また、本発明の I P s e c 設定方法では、上記構成において、要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 処理装置の通信相手の I P s e c 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、各 I P s e c 処理装置間に適用する I P s e c のポリシーの設定がそれらの装置ではほぼ同時に行われることとなり、ポリシー設定後の暗号化や復号を滞りなく行うことが可能となる。これによって、送信先の I P s e c 処理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【0032】

さらに、本発明の I P s e c 設定方法では、上記構成において、I P s e c 設定サーバが要求起動メッセージの送信時にそれに応答した要求メッセージを受信しなければ、送信元の I P s e c 処理装置に応答なしエラーメッセージを送信するので、送信元の I P s e c 処理装置で対向装置の不存在を認識することが可能となる。

【0033】

さらにまた、本発明の I P s e c 設定方法は、上記構成において、I P s e c

の暗号化や認証に使用するための共有秘密鍵を各 I P s e c 処理装置が I P s e c 設定サーバから取得することによって、複雑な鍵交換演算を省略し、I P s e c 処理開始までの時間を短縮するものである。

【 0 0 3 4 】

より具体的に説明すると、本発明の I P s e c 設定方法では、I P s e c 設定サーバが各 I P s e c 処理装置間に適用する I P s e c のポリシーを記憶している。送信元の I P s e c 処理装置が相手先の I P s e c 処理装置にデータ通信パケットを送信する場合、送信元の I P s e c 処理装置は必要な設定を I P s e c 設定サーバに要求する。要求を受信した I P s e c 設定サーバは相手先の I P s e c 処理装置に対しても設定を要求するように指示する。

【 0 0 3 5 】

相手先の I P s e c 処理装置からの要求を受信した時点で、I P s e c 設定サーバは登録済みのポリシーと、送信元及び相手先の両方の I P s e c 処理装置から通知された S P I (S e c u r i t y P a r a m e t e r s I n d e x : セキュリティパラメータインデックス)、及び I P s e c 設定サーバが生成した共有秘密鍵をそれぞれの I P s e c 処理装置に送信する。この時点で送信元及び相手先の両方の I P s e c 処理装置には I P s e c 処理に必要な情報がすべて揃い、I P s e c 処理を実行することが可能となる。尚、設定情報の送受信については、従来の I P s e c によって保護することによって、第 3 者による盗聴を防ぐ。

【 0 0 3 6 】

このように、本発明では、I P s e c ポリシーを I P s e c 設定サーバで一括して管理することによって、全体の設定数を削減すると同時に、2 拠点間での設定内容が異なるために発生する通信障害を防止することが可能となる。

【 0 0 3 7 】

また、本発明では、要求起動メッセージを送信しているので、要求メッセージの送信元の I P s e c 処理装置に対向する I P s e c 処理装置ではその送信元の I P s e c 処理装置での I P s e c のポリシーの設定とほぼ同時に I P s e c のポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元の I P

s e c 処理装置がパケットを暗号化して送信すると、対向する I P s e c 処理装置では送信元の I P s e c 処理装置からのパケットを復号して受取ることが可能となる。これによって、送信先の I P s e c 処理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【0038】

さらに、本発明では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向する I P s e c 処理装置から送られてこなければ、送信元の I P s e c 処理装置に対して応答なしエラーメッセージが送信されるので、送信元の I P s e c 処理装置で対向装置の不存在を即座に認識することが可能となる。

【0039】

さらにまた、本発明では、共有秘密鍵の取得に I K E (I n t e r n e t K e y E x c h a n g e : 自動鍵管理プロトコル) を用いないため、I K E で使用する D i f f i e - H e l l m a n の演算をする必要がない。したがって、D i f f i e - H e l l m a n の演算を必要とする従来の手法と比較して、I P s e c 処理開始までの時間を短縮することが可能となる。

【0040】

従来の手法では I K E の S A (S e c u r i t y A s s o c i a t i o n) を更新するために D i f f i e - H e l l m a n の演算が定期的に発生し、そのたびに演算負荷が発生する。I P s e c による通信相手が多いほど、I K E の S A を更新する機会も増えるので、演算負荷も増加し、I P s e c 処理装置全体の処理性能が低下する。

【0041】

これに対し、本発明では、I P s e c 処理装置と I P s e c 設定サーバとの間以外の通信については、D i f f i e - H e l l m a n の演算を行わないため、従来の手法と比較して、演算負荷も軽減することが可能となる。

【0042】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例による I P s e c (I n t e r n e t P r o t o c o l s e c u r i t

y protocol) によるネットワークの構成を示すブロック図である。図 1 において、本発明の一実施例によるネットワークは互いに IPsec 適用通信を実施しようとする複数台の IPsec 処理装置 2a~2f がインターネット 100 を介して接続され、同じくインターネット 100 上に IPsec 設定サーバ 1 を接続して構成している。尚、図 1 に示すように、IPsec 処理装置 2a~2f はそれぞれの背後に存在するプライベートネットワーク 201~204 を IPsec による通信によって相互に接続するルータであってもよいし、自分自身の通信に IPsec を適用するパーソナルコンピュータ（以下、パソコンとする）であってもよい。

【0043】

図 2 に図 1 の IPsec 設定サーバ 1 の構成を示すブロック図である。図 2 において、IPsec 設定サーバ 1 はインタフェース (I/F) 部 11 と、IPsec 処理部 12 と、SPD (Security Policy Database) 13 と、SAD (Security Association Database) 14 と、要求処理部 15 と、配布ポリシー記憶部 16 と、管理テーブル 17 と、乱数生成器 18 と、タイマ 19 と、記録媒体 20 とから構成されている。ここで、IPsec 設定サーバ 1 は主にコンピュータから構成され、コンピュータが記録媒体 20 に格納されたプログラムを実行することで上記の各部の動作が実現される。

【0044】

インタフェース部 11 はインターネット 100 に接続され、インターネット 100 を介したデータ通信を行う。IPsec 処理部 12 はインタフェース部 11 から受信したデータ通信パケットに対して IPsec 処理を実施する。

【0045】

SPD 13 は IPsec 処理部 12 から参照され、IPsec を適用するためのポリシーを記録している。SAD 14 は IPsec 処理部 12 から参照され、個々の通信に対して IPsec 処理を実施するために必要な SA (Security Association) を記録している。

【0046】

要求処理部 15 はインタフェース部 11 経由で IPsec 処理装置 2a ~ 2f から設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部 16 は要求処理部 15 から参照され、要求された設定を決定するために必要な IPsec ポリシーが記憶されている。管理テーブル 17 は要求処理部 15 から参照、設定され、設定要求を受けた各々の SA 通信に関する情報が記憶されている。

【0047】

乱数生成器 18 は要求処理部 15 からの要求によって乱数を生成する。タイマ 19 は要求処理部 15 から要求され、時間を計測する。これらの中で IPsec 処理部 12、SAD 14、SPD 13 は IPsec 設定サーバ 1 が IPsec 処理装置 2 との通信を IPsec によって保護するために必要となるだけであり、従来の IPsec の機構と同一である。

【0048】

インタフェース部 11 はインターネット 100 からデータ通信パケットを受信すると、そのデータ通信パケットを IPsec 処理部 12 に転送し、また IPsec 処理部 12 から転送されたデータ通信パケットをインターネット 100 に送信する。

【0049】

IPsec 処理部 12 はインターネット 100 から受信した IPsec 適用済みのデータ通信パケットに対して SAD 14 や SPD 13 の記憶内容を基に IPsec の復号処理を行い、IPsec 適用前の状態にして要求処理部 15 に転送する。また、IPsec 処理部 12 は要求処理部 15 から受信したデータ通信パケットに対して SPD 13 及び SAD 14 の記憶内容にしたがって IPsec 処理を適用し、インタフェース部 11 に転送する。IPsec 処理部 12 は IPsec 設定サーバ 1 と IPsec 処理装置 2a ~ 2f との間の通信を保護するために必要な機構であり、従来の IPsec と全く同じものである。

【0050】

図 3 は図 2 の配布ポリシー記憶部 16 の記憶内容を示す図である。図 3 において、配布ポリシー記憶部 16 には配布ポリシーを特定するためのアドレスペア欄

と、配布する I P s e c ポリシーを設定する配布ポリシー欄とがある。配布ポリシー記憶部 16 の配布ポリシーに設定可能なパラメータは I P s e c プロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、S A の有効期間である。

【0051】

図3に示す例では、I P s e c 処理装置 2 a - I P s e c 処理装置 2 b 間の通信に適用する I P s e c ポリシー、I P s e c 処理装置 2 d - I P s e c 処理装置 2 e 間の通信に適用する I P s e c ポリシーが設定されている。尚、配布ポリシー記憶部 16 には予めすべての項目をユーザが設定しておく必要がある。また、一度設定した後は動作中に自動的に書換えられることはない。

【0052】

I P s e c 処理装置 2 a - I P s e c 処理装置 2 b 間の配布ポリシーとしては、I P s e c プロトコルに「E S P (E n c a p s u l a t i n g S e c u r i t y P a y l o a d : カプセル化セキュリティペイロード)」、カプセル化モードに「トンネルモード」、暗号化アルゴリズムに「D E S - C B C (D a t a E n c r y p t i o n S t a n d a r d - C i p h e r B l o c k C h a i n i n g)」、認証アルゴリズムに「H M A C (H a s h i n g M e s s a g e A u t h e n t i c a t i o n C o d e) - M D 5 - 9 6」、S A の有効期間に「3 6 0 0 秒」が設定されている。

【0053】

また、I P s e c 処理装置 2 d - I P s e c 処理装置 2 e 間の配布ポリシーとしては、I P s e c プロトコルに「E S P」、カプセル化モードに「トランスポートモード」、暗号化アルゴリズムに「3 D E S - C B C」、認証アルゴリズムに「H M A C - S H A - 1 - 9 6」、S A の有効期間に「3 6 0 0 秒」が設定されている。

【0054】

従来の手法では適用する I P s e c ポリシーの内容についてそれぞれの I P s e c 処理装置 2 a ~ 2 f に個別に同一の設定を入力する必要があるが、本発明の手法では I P s e c 処理装置 2 a ~ 2 f 間の I P s e c 通信に対しては配布ポリ

シー記憶部 16 のみに I P s e c ポリシーを設定すればよいため、誤ってそれぞれの I P s e c 処理装置 2 a ~ 2 f に異なる設定をしてしまう事故を回避することができると同時に、ユーザが実際に入力する設定の数も減らすことができる。

【0055】

図 4 は図 2 の管理テーブル 17 の記憶内容を示す図である。図 4 において、管理テーブル 17 には I P s e c 処理装置 2 a ~ 2 f から送られる要求メッセージに含まれる要求元アドレス、相手先アドレス、ID、S P I (S e c u r i t y P a r a m e t e r I n d e x : セキュリティパラメータインデックス) をそれぞれ記録する要求元アドレス欄、相手先アドレス欄、要求 ID 欄、S P I 欄と、当該通信用の I P s e c 処理に必要なパラメータ群を記録する設定パラメータ欄とがある。このうち、設定パラメータ欄には当該通信に適用するポリシー及び当該通信用 S A の構築に必要なパラメータからなる S A パラメータが設定される。

【0056】

図 5 は図 4 の S A パラメータの内容を示す図である。図 5 において、S A パラメータは I P s e c プロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限、暗号鍵、認証鍵、I V (I n i t i a l i z a t i o n V e c t o r) と、当該通信の受信側 I P s e c 処理装置 2 a ~ 2 f で使用する S P I 値からなる。

【0057】

1 個の I P s e c 通信に対して、通信を行う両端の I P s e c 処理装置 2 a ~ 2 f から要求が発生するため、管理テーブル 17 の 1 個のエントリには要求元アドレス、相手先アドレス、要求 ID、S P I は 2 個ずつ存在する。また、同一の I P s e c 通信であっても、S A の有効期限満了に備えて新しい S A が要求される場合があり、この場合には管理テーブル 17 には新しい S A のために新しく 1 個のエントリが登録される。尚、管理テーブル 17 の内容はすべて要求処理部 15 によって自動的に設定されるため、管理テーブル 17 の内容をユーザが直接設定する必要はない。

【0058】

管理テーブル 17 を参照することで、IPsec 処理装置 2a～2f に配布する設定パラメータを得ることができる。設定パラメータ内の SA パラメータは IPsec 通信を実施するそれぞれの IPsec 処理装置 2a～2f からの要求メッセージを受信することで確定するため、片方の IPsec 処理装置 2a～2f からしか要求メッセージを受信していない場合には、相手側の要求 ID 欄及び SPI 欄が空欄となり、設定パラメータ欄の SA パラメータも空欄となる。但し、適用ポリシーについては片方の IPsec 処理装置 2a～2f から要求メッセージを受信するだけで確定するため、片方の IPsec 処理装置 2a～2f から要求メッセージを受信するだけで、適用するポリシーが設定される。

【0059】

図 4 に示す例では、1 番目のエントリに IPsec 処理装置 2a と IPsec 処理装置 2b との通信に適用されるポリシー及び SA パラメータがそれぞれ登録されている。2 番目のエントリには同じく IPsec 処理装置 2a と IPsec 処理装置 2b との通信に適用されるポリシーが登録されているが、IPsec 処理装置 2b から対応する設定要求メッセージを受信していないため SA パラメータが確定していない。

【0060】

図 5 に図 4 内の SA パラメータ (a) の内容を示す。SA パラメータは配布ポリシーの内容、設定要求メッセージで通知された SPI、及び乱数生成器 18 から得られる乱数を基に要求処理部 15 によって生成される。

【0061】

要求処理部 15 は IPsec 処理装置 2a～2f から要求メッセージを受信して、IPsec 処理装置 2a～2f に要求起動メッセージや配布メッセージ、エラーメッセージを送信する。

【0062】

図 6 は本発明の一実施例による要求メッセージの一例を示す図である。図 6 において、要求メッセージには要求メッセージを他の要求メッセージと区別するための ID 「1001」と、要求メッセージを送信した IPsec 処理装置 2a～2f のアドレスを示す要求元アドレス「IPsec 処理装置 2a」と、相手とな

る I P s e c 処理装置 2 a ~ 2 f のアドレスを示す相手先アドレス「I P s e c 処理装置 2 b」と、要求元で使用する S P I の値「5 1 0 0」とが含まれている。

【0 0 6 3】

尚、本実施例では 2 台の I P s e c 処理装置 2 a ~ 2 f 間に存在する I P s e c 通信を 1 種類に限定しているため、両方の I P s e c 処理装置 2 a ~ 2 f のアドレスが決まれば、適用する I P s e c ポリシーを一意に特定することができる。したがって、要求メッセージには I P s e c 通信の両端のアドレスを設定している。これ以外に、2 台の I P s e c 処理装置 2 a ~ 2 f 間に複数の I P s e c 通信を設定したい場合が考えられる。そのような場合には、それぞれの I P s e c 通信を特定するために必要な情報（例えば、プロトコル番号やポート番号等）を要求メッセージに設定する。

【0 0 6 4】

図 7 は本発明の一実施例による配布メッセージの一例を示す図であり、図 8 は本発明の一実施例による要求起動メッセージの一例を示す図であり、図 9 は本発明の一実施例による該当なしエラーメッセージの一例を示す図であり、図 1 0 は本発明の一実施例による内容不一致エラーメッセージの一例を示す図であり、図 1 1 は本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【0 0 6 5】

図 1 2 及び図 1 3 は本発明の一実施例による I P s e c 設定サーバ 1 の動作を示すフローチャートである。これら図 1 ~ 図 1 3 を参照して本発明の一実施例による I P s e c 設定サーバ 1 の動作について説明する。まず、要求処理部 1 5 が要求メッセージを受信した場合の動作について説明する。

【0 0 6 6】

要求処理部 1 5 は I P s e c 処理装置 2 a ~ 2 f から要求メッセージを受信すると（図 1 2 ステップ S 1）、管理テーブル 1 7 の中から要求メッセージに含まれる要求元アドレス、相手先アドレス、I D が一致するエントリを検索する（図 1 2 ステップ S 2）。

【0067】

要求処理部15は一致するエントリが見つかり、一致したエントリのSP Iが要求メッセージに含まれるSP Iと一致するかどうかを確認する（図12ステップS3）。要求処理部15はSP Iが一致しなければ、IPsec処理装置2a～2fに内容不一致エラーメッセージを送信する（図12ステップS8）。

【0068】

この時、内容不一致エラーメッセージには要求メッセージに含まれるID、要求元アドレス、相手先アドレスと、エントリ一覧とを設定する。エントリ一覧には管理テーブル17に含まれるエントリの中で、要求元アドレスと相手先アドレスとが一致するすべてのエントリを設定する。但し、エントリ一覧に設定する項目は各エントリの要求IDとそのエントリで使用する要求元アドレス用のSP Iだけである。

【0069】

IPsec処理装置2a～2fは内容不一致エラーメッセージを受信することでIPsec設定サーバ1が管理している設定情報と、IPsec処理装置2a～2fが把握している設定情報との差分を知ることができる。

【0070】

この内容不一致エラーメッセージの一例を図10に示す。図10において、IPsec設定サーバ1上においてIPsec処理装置2aとIPsec処理装置2bとの通信用にすでに「1001」，「1002」という要求IDによって設定情報が生成されており、そこで使用しているSP Iの値がそれぞれ「5100」，「5110」であることがわかる。

【0071】

要求処理部15は管理テーブル17の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、IDと一致するエントリが見つかってSP Iの内容も一致した場合、管理テーブル17内の当該エントリの相手側の要求ID欄を確認する（図12ステップS4）。

【0072】

要求処理部15は相手側の要求ID欄が設定されている場合、すでに管理テー

ブル 17 の設定パラメータ欄が確定しているため、要求メッセージの送信元に配布メッセージを送信する（図 12 ステップ S5）。配布メッセージには要求メッセージに含まれる要求元アドレス、送信元アドレス、ID を設定し、設定パラメータには管理テーブル 17 内の配布ポリシーと SA パラメータとを設定する。この場合は、すでに返送すべき設定パラメータがすべて確定している場合である。

【0073】

この配布メッセージの一例を図 7 に示す。図 7 に示す例では、設定パラメータには配布ポリシー（a）と SA パラメータ（a）、SA パラメータ（b）が設定されている。IPsec 処理装置 2a は配布ポリシー（a）と SA パラメータ（a）、SA パラメータ（b）とを使用して双方向の IPsec 通信を実施することができる。

【0074】

要求処理部 15 は管理テーブル 17 の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、ID と一致するエントリが見つかって SPI の内容も一致した場合で、相手側の要求 ID 欄が設定されていなかった場合、そのまま処理を終了する（図 12 ステップ S6）。この場合には、すでに IPsec 処理装置 2a ～ 2f から同一の要求メッセージを受信しているが、相手側の情報がないため、相手側の情報を待っている状態である。

【0075】

要求処理部 15 は管理テーブル 17 の中に要求元アドレス、相手先アドレス、ID が一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレス、相手先アドレス、SPI をキーにして管理テーブル 17 を検索する（図 12 ステップ S7）。

【0076】

要求処理部 15 は一致するエントリが見つかり、要求メッセージの送信元に内容不一致エラーメッセージを送信して処理を終了する（図 12 ステップ S8）。これは既に IPsec 設定サーバ 1 に登録済みの SPI を重複して使用して IPsec 処理装置 2a ～ 2f が新しい設定パラメータを要求した場合である。IPsec 処理装置 2a ～ 2f は内容不一致エラーメッセージを受信することで、

S P I の重複を検出し、重複しない S P I を選択することができる。

【0077】

要求処理部 15 は管理テーブル 17 の中に要求元アドレス、相手先アドレス、I D が一致するエントリがなく、S P I の重複も検出されなければ、要求メッセージに含まれる要求元アドレスと相手先アドレスとをキーにして管理テーブル 17 を検索する（図 12 ステップ S 9）。この時、要求処理部 15 は要求 I D 欄が空欄のエントリを検索する。

【0078】

一致するエントリが存在した場合には、すでに相手側の I P s e c 処理装置 2 a ~ 2 f から当該通信に対する要求メッセージが送信されており、設定パラメータの適用ポリシーまで確定している状態である。要求処理部 15 は空欄になっている要求 I D 欄及び S P I 欄に要求メッセージに設定されている I D 及び S P I を設定し、設定パラメータ欄の適用ポリシーで示されるポリシーにしたがって、それぞれの方向用に S A パラメータを生成する。

【0079】

具体的に述べると、I P s e c プロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限については適用ポリシーと同一の内容を設定し、暗号化鍵、認証鍵、I V については乱数生成器 18 から乱数を取得して値を決定し、受信側 S P I 欄には受信側の I P s e c 処理装置 2 a ~ 2 f が使用する S P I の値を設定する。

【0080】

要求処理部 15 はそれぞれの方向用の S A パラメータが生成できたら、管理テーブル 17 の設定パラメータ欄に登録する（図 12 ステップ S 10）。要求処理部 15 は管理テーブル 17 に S A パラメータを登録すると、要求メッセージの送信元である I P s e c 処理装置 2 a ~ 2 f の要求 I D と、設定パラメータを設定した配布メッセージを I P s e c 処理装置 2 a ~ 2 f に送信すると同時に、相手先となる I P s e c 処理装置 2 a ~ 2 f に対しても、相手先の要求 I D を含む配布メッセージを送信する（図 12 ステップ S 11）。

【0081】

また、要求処理部 15 はタイマ 19 を使用して S A パラメータの有効期限と同じ時間を計測し、タイマ 19 が満了した時点で、管理テーブル 17 の当該エントリを削除する。

【0082】

要求処理部 15 は管理テーブル 17 の中に要求元アドレスと要求 I D とが一致するエントリがなく、要求元アドレスと相手先アドレスとをキーとした検索でも一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレスと相手先アドレスとの組をキーにして配布ポリシー記憶部 16 を検索する（図 13 ステップ S 21）。

【0083】

要求処理部 15 は該当するエントリが見つからなければ、I P s e c 処理装置 2 a ~ 2 f に該当なしエラーメッセージを送信する（図 13 ステップ S 26）。該当なしエラーメッセージには要求メッセージに含まれていた I D、要求元アドレス、相手先アドレスを設定する。この該当なしエラーメッセージの一例を図 9 に示す。

【0084】

要求処理部 15 は配布ポリシー記憶部 16 内に一致するエントリが存在した場合、管理テーブル 17 の新しいエントリの要求元アドレス、相手先アドレス、要求 I D、S P I 欄にそれぞれ要求メッセージに含まれる要求元アドレス、相手先アドレス、I D、S P I を設定する。同一エントリのもう一つの要求元アドレスには要求メッセージの相手先アドレスを、相手先アドレスには要求メッセージの要求元アドレスを設定し、要求 I D、S P I は空欄とする。

【0085】

また、要求処理部 15 は配布ポリシー記憶部 16 の該当エントリに含まれる配布ポリシーを管理テーブル 17 の設定パラメータ欄に設定する（図 13 ステップ S 22）。この時点で、S A パラメータを生成するために必要なパラメータ群のうち、暗号化鍵、認証鍵等の共有秘密鍵、相手先 I P s e c 処理装置 2 a ~ 2 f で使用する S P I 以外のパラメータがすべて確定する。共有秘密鍵は乱数生成器 19 から得られる乱数を使用するため、相手先の S P I さえ確定すれば、S A パ

ラメータを生成することが可能となる。

【 0 0 8 6 】

要求処理部 1 5 は配布ポリシー記憶部 1 6 内に一致するエントリが存在し、管理テーブル 1 7 に要求元の I P s e c 処理装置 2 a ～ 2 f からの要求に応じてエントリを登録した後、相手先の I P s e c 処理装置 2 a ～ 2 f に対して要求起動メッセージを送信する（図 1 3 ステップ S 2 3）。要求起動メッセージには要求メッセージの要求元アドレスを設定する。この要求起動メッセージの一例を図 8 に示す。

【 0 0 8 7 】

要求処理部 1 5 は要求起動メッセージを送信すると、5 秒間隔で要求起動メッセージの送信を繰り返し、要求起動メッセージの送信先の I P s e c 処理装置 2 a ～ 2 f から管理テーブル 1 7 の該当エントリに対応する要求メッセージを受信するか、要求起動メッセージを 6 回送信すると、要求起動メッセージの送信を停止する。繰り返し送信することによって、1 個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【 0 0 8 8 】

要求処理部 1 5 は 6 回の要求起動メッセージ送信によって送信を停止した場合（図 1 3 ステップ S 2 4）、管理テーブル 1 7 から該当エントリを削除し（図 1 3 ステップ S 2 7）、要求メッセージの送信元の I P s e c 処理装置 2 a ～ 2 f には応答なしエラーメッセージを送信する（図 1 3 ステップ S 2 8）。応答なしエラーメッセージには、I P s e c 処理装置 2 a ～ 2 f からの要求メッセージに含まれていた I D、要求元アドレス、相手先アドレスを設定する。この応答なしエラーメッセージの一例を図 1 1 に示す。

【 0 0 8 9 】

要求処理部 1 5 は要求起動メッセージに対して、管理テーブル 1 7 の該当エントリに対応する要求メッセージを受信した場合（図 1 3 ステップ S 2 4）、要求起動メッセージの送信を停止し、要求メッセージ受信時の動作を行う（図 1 3 ステップ S 2 5）。

【 0 0 9 0 】

タイマ 19 は要求処理部 15 に依頼されて時間を計測し、指定された時間が経過したら要求処理部 15 に通知する。タイマ 19 は同時に複数の時間を計測することができる。

【0091】

上記のように、要求起動メッセージを送信しているので、要求メッセージの送信元の IPsec 処理装置に対向する IPsec 処理装置ではその送信元の IPsec 処理装置での IPsec のポリシーの設定とはほぼ同時に IPsec のポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元の IPsec 処理装置がパケットを暗号化して送信すると、対向する IPsec 処理装置では送信元の IPsec 処理装置からのパケットを復号して受取ることができる。よって、ポリシー設定後の暗号化や復号を滞りなく行うことができる。

【0092】

この場合、パケットの復号ができなくてそのパケットを破棄したり、パケットの復号を誤って行ったりすることがないので、送信先の IPsec 処理装置において送信元からのパケットを取りこぼしなく受取ることができる。

【0093】

また、要求起動メッセージの送信時にそれに応答した要求メッセージを対向する IPsec 処理装置から受信しなければ、送信元の IPsec 処理装置に対して応答なしエラーメッセージを送信するので、送信元の IPsec 処理装置では対向装置の不存在を即座に認識することができる。

【0094】

図 14 は図 1 の IPsec 処理装置 2a～2f の構成を示すブロック図である。図 14 においては IPsec 処理装置 2a～2f をまとめて IPsec 処理装置 2 としており、IPsec 処理装置 2a～2f は IPsec 処理装置 2 と同様の構成である。

【0095】

IPsec 処理装置 2 は主にコンピュータから構成され、IPsec 設定サーバ 1 を利用する。つまり、IPsec 処理装置 2 はインタフェース部 (I/F) 21、22 と、IPsec 処理部 23 と、SPD 24 と、SAD 25 と、設定管

理部 26 と、ルーティング部 27 と、記録媒体 28 とを具備し、上記の各部の動作はコンピュータが記録媒体 28 のプログラムを実行することで実現される。

【0096】

インタフェース部 21 はプライベートネットワーク 200（図 1 のプライベートネットワーク 201～204）に接続され、プライベートネットワーク 200 とのデータ通信を行う。インタフェース部 22 はインターネット 100 に接続され、インターネット 100 を介したデータ通信を行う。

【0097】

IPsec 処理部 23 はインタフェース部 21，22 から受信したデータ通信パケットに対して IPsec 処理を実施する。設定管理部 26 は IPsec 処理部 23 に依頼され、必要な設定を IPsec 設定サーバ 1 に要求する。

【0098】

SPD 24 は IPsec 処理部 23 及び設定管理部 26 から参照され、IPsec を適用するためのポリシーを記録している。SAD 25 は IPsec 処理部 23 と設定管理部 26 とから参照され、個々の通信に対して IPsec 処理を実施するために必要な SA を記録している。ルーティング部 27 は IPsec 処理部 23 と設定管理部 26 との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【0099】

IPsec 処理装置 2 の構成は図 31 に示す従来の IPsec 処理装置の構成と比較すると、IPsec 処理装置 2 では設定管理部 26 が追加されている点異なる。また、後述するように、SPD 24 に新しい項目がされた点と、IPsec 処理部 23 に新しい動作が加えられた点とが異なる。

【0100】

インタフェース部 21 はプライベートネットワーク 200 からデータ通信パケットを受信して IPsec 処理部 23 に転送し、また IPsec 処理部 23 から転送されたデータ通信パケットをプライベートネットワーク 200 に送信する。

【0101】

インタフェース部 22 はインターネット 100 からデータ通信パケットを受信し

て I P s e c 処理部 2 3 に転送し、また I P s e c 処理部 2 3 から転送されたデータ通信パケットをインターネット 1 0 0 に送信する。

【 0 1 0 2 】

S P D 2 4 には個々の S P D エントリを識別し、優先順位を明確にするための I D 欄と、トラヒックを選択するためのセクタ欄、選択されたトラヒックに対する処理欄、I P s e c 処理を適用する場合の I P s e c のパラメータ情報等を記録する I P s e c 適用ポリシー欄、及び S P D 検索時に I P s e c 設定サーバ 1 に設定を要求するか否かを判断するための設定要求用相手アドレス欄が存在する。

【 0 1 0 3 】

図 1 5 は図 1 4 の S P D 2 4 の内容を示す図である。図 1 5 において、S P D 2 4 は設定要求用相手アドレス欄が追加されている以外は通常の I P s e c で用いられる S P D と同一のものである。尚、S P D 2 4 は送信用と受信用とが存在する。

【 0 1 0 4 】

S P D 2 4 は I P s e c 処理部 2 3 がデータ通信パケットを受信した場合に、そのパケットの扱いを決定するために用いられる。I P s e c 処理部 2 3 は I P s e c が適用されていないデータ通信パケットを受信すると、S P D 2 4 のセクタ欄と比較して一致するエントリを探す。一致するエントリが発見されると、処理欄にしたがって当該パケットの扱いを決定する。

【 0 1 0 5 】

処理欄には“ I P s e c 適用”、“通過”、“廃棄”のいずれかが格納される。特に、“ I P s e c 適用”の処理となった場合には、I P s e c ポリシー欄の内容にしたがって引き続き I P s e c の処理が行われる。

【 0 1 0 6 】

本実施例では S P D 2 4 に存在する設定要求用相手アドレス欄において、処理欄が“ I P s e c 適用”となった場合にその I P s e c 適用ポリシー欄を I P s e c 設定サーバ 1 に要求するか否かを判断するために使用すると同時に、I P s e c 設定サーバ 1 に設定を要求する場合に、要求する設定パラメータを特定する

ための識別子としても使用する。

【0107】

尚、SPD24の内容は標準のIPsecと同様に、基本的に予めすべて設定しておく必要があるが、設定要求用相手アドレスを設定したエントリについてはIPsec適用ポリシーを省略することが可能である。この場合には設定管理部26がIPsec設定サーバ1から必要なIPsec適用ポリシー情報を入手し、自動的にSPD24のIPsec適用ポリシー欄を設定する。この時、IPsec設定サーバ1との通信を暗号化するための設定だけは適用ポリシーを省略することはできない。

【0108】

図15に示す例では、IPsec処理装置2a自身からIPsec設定サーバ1宛のパケットに対して適用ポリシー(z)にしたがってIPsec処理を実施し、プライベートネットワーク202宛のパケット、及びプライベートネットワーク203宛のパケットに対してIPsec処理を適用するが、そのポリシーはIPsec設定サーバ1から取得し、それ以外のすべてのパケットはIPsec処理を適用せずに通過させる設定となっている。

【0109】

図16は図15に示すSPD24の適用ポリシー(z)の一例を示す図である。図16において、IPsec適用ポリシーにはIPsec通信で使用するプロトコルやカプセル化モード、暗号化アルゴリズム、認証アルゴリズム等、適用するIPsec処理を特定するために必要な情報が設定される。

【0110】

図16に示す例では、暗号化アルゴリズムに「AES-CBC」、認証アルゴリズムに「HMAC-SHA-1-96」を使用してESPの「トランスポートモード」を適用することと、SAの有効期間が「3600秒」であることが示されている。尚、使用するプロトコルや暗号化アルゴリズム等によって必要となるパラメータが異なるため、それぞれの適用ポリシーにおいては図16に示すパラメータ以外のパラメータが現れる場合や、図16の中の一部のパラメータが存在しない場合もある。

【0111】

従来の IPsec では適用ポリシーを IPsec 処理装置に予めすべてユーザが設定しておく必要があるが、前項で述べた通り、本実施例の SPD24 では適用ポリシーの設定を省略することが可能である。その場合には設定管理部 26 によって IPsec 設定サーバ 1 から取得した IPsec 適用ポリシーが自動的に設定される。

【0112】

尚、IKE を使用する場合には IKE 自身に必要となるパラメータが SPD24 の IPsec 適用ポリシーとは独立して存在する。しかしながら、本実施例の観点から見ると、IPsec 通信を行うために、本来ユーザが設定しなければならないパラメータであって、本実施例の IPsec 設定サーバ 1 を使用することによって省略可能なパラメータである、という点において IPsec 適用ポリシーと同等である。そこで、説明を容易にするため、SPD24 の IPsec 適用ポリシーが IKE を使用するポリシーの場合には、そのポリシーの中に IKE 用のパラメータもすべて含まれているものとして扱う。そのため、図 16 に示す例では IKE 用の設定パラメータも含まれている。実際の構成においては依然として IKE 自身の設定は IPsec 適用ポリシーとは独立である。

【0113】

図 17 は図 14 の SAD25 の内容を示す図である。図 17 において、SAD25 には個々の IPsec 通信に必要となる SA が登録される。すなわち、SAD25 は SA を管理するためのデータベースである。

【0114】

SPD24 の IPsec 適用ポリシーでは、適用する IPsec 処理（どのような種類の IPsec 処理を施すか）を示すための情報が示されるが、実際に IPsec 処理を行うためには追加の情報が必要となる。

【0115】

例えば、IKE を使用する場合には、IPsec 処理で使用する暗号化鍵や認証鍵を相手 IPsec 処理装置と交換し、それらの値を使用することで初めて一つの IPsec 処理が実施することができる。このように、一つの IPsec 処

理を実施するために必要なパラメータ群を S A と呼ぶ。

【0116】

S A D 2 5 には個々の S A D エントリを識別するための I D と、 I P s e c 通信の相手アドレスを示す終点アドレスと、 I P s e c 通信で使用する I P s e c プロトコルと、個々の S A に固有の識別子である S P I 及びその他の S A パラメータとによって構成される。

【0117】

S A D 2 5 は設定管理部 2 6 あるいは I P s e c 処理部 2 3 によって自動的に設定されるため、S A D 2 5 をユーザが直接設定する必要はない。尚、S A D 2 5 は標準の I P s e c で用いられる S A D と同一のものであり、送信用と受信用とが存在する。

【0118】

図 1 7 に示す例では、1 番目のエントリに I P s e c 処理装置 2 a と I P s e c 処理装置 2 b との間の S A が、2 番目のエントリに I P s e c 処理装置 2 a と I P s e c 設定サーバ 1 との間の S A が登録されている。

【0119】

図 1 8 は図 1 4 の I P s e c 処理部 2 3 の処理動作を示すフローチャートであり、図 1 9 及び図 2 0 は図 1 4 の設定管理部 2 6 の処理動作を示すフローチャートである。これら図 1 8 ～図 2 0 を参照して I P s e c 処理装置 2 a ～2 f の動作について説明する。

【0120】

I P s e c 処理部 2 3 はプライベートネットワーク 2 0 0 からインターネット 1 0 0 宛のデータ通信パケットを受信すると（図 1 8 ステップ S 3 1）、データ通信パケットと S P D 2 4 のセレクトラ欄とを比較して該当するエントリを検索する（図 1 8 ステップ S 3 2）。該当するエントリの設定要求用相手アドレス欄が空欄の場合には、従来の I P s e c と同一の動作である（図 1 8 ステップ S 3 3）。

【0121】

尚、この従来の I P s e c の動作によって、I P s e c 処理装置 2 と I P s e

c 設定サーバ 1 とのメッセージの送受信は保護される。すなわち、予め通常の IPsec の方法に従って IPsec 処理装置 2 と IPsec 設定サーバ 1 との間の通信については SPD 24 に登録しておく。

【0122】

IPsec 処理部 23 は SPD 24 の検索で該当するエントリの設定要求用相手アドレス欄が設定されていた場合で、IPsec 適用ポリシー欄が設定されている場合、さらに SAD 25 から当該通信用の SA を検索する（図 18 ステップ S34）。当該通信用の SA が存在する場合には、従来の IPsec と同一の動作となり、SA の内容にしたがってデータ通信パケットに IPsec 処理を適用する（図 18 ステップ S33）。

【0123】

IPsec 処理部 23 は SPD 24 の検索で該当するエントリの設定要求用相手アドレス欄が設定されており、IPsec 適用ポリシー欄も設定されている場合で、SAD 25 に該当エントリがない場合、あるいはそもそも IPsec 適用ポリシー欄が設定されていない場合、当該データ通信パケットの処理を一時中断し、設定管理部 26 に設定サーバから設定を取得するように依頼する（図 18 ステップ S35）。この時、設定管理部 26 には SPD 24 の当該エントリの ID を通知する。

【0124】

IPsec 処理部 23 は設定管理部 26 に依頼した後、設定管理部 26 から結果が通知されるまで同一の SPD エントリに対する依頼は行わない。IPsec 処理部 23 は設定管理部 26 から設定完了の通知を受けると（図 18 ステップ S36）、データ通信パケットの IPsec 処理を再開する（図 18 ステップ S33）。この時点では、必要なポリシー及び SA が設定管理部 26 によって設定されており、従来通りの IPsec 処理を実施するのみとなる。

【0125】

IPsec 処理部 23 は設定管理部 26 から設定失敗の通知を受けると（図 18 ステップ S33）、一時中断していたデータ通信パケット処理を中止する（図 18 ステップ S37）。

【0126】

IPsec 処理部 23 はインターネット 100 からプライベートネットワーク 200 宛の IPsec 適用済みデータ通信パケットを受信した場合、従来の IPsec と同様に動作する。すなわち、IPsec 処理部 23 は SAD 24 から該当するエントリを検索し、一致するエントリが存在した場合、その内容にしたがって IPsec の復号処理を実施する。IPsec 処理部 23 は一致するエントリが存在しない場合、そのデータ通信パケットを廃棄する。

【0127】

IPsec 処理部 23 は従来の IPsec と同様に、SAD 25 内の各 SA エントリの有効期限を確認し、有効期限が満了する前に新しい SA の確立を行う。この時、当該 SA が IPsec 設定サーバ 1 によって生成された SA だった場合、IPsec 処理部 23 は設定管理部 26 に IPsec 設定サーバ 1 から設定を取得するように依頼する。

【0128】

設定の取得を依頼する時、IPsec 処理部 23 は設定管理部 26 に当該 SA に対応する SPD 24 エントリの ID を通知する。設定管理部 26 からは依頼に対する結果が通知されるが、IPsec 処理部 23 はその結果の通知を無視する。

【0129】

設定管理部 26 は IPsec 処理部 23 から設定取得の依頼を受けると（図 19 ステップ S41）、通知された SPD 24 のエントリ用の要求メッセージを生成する（図 19 ステップ S42）。要求メッセージには ID と、要求元アドレスと、相手先アドレスと、要求元で使用する SPI の値とを設定する。ID には他の要求メッセージと重複しない任意の数値を設定し、SPI には IPsec 通信において自己が使用するつもり SPI を設定する。要求元アドレスには IPsec 処理装置 2 のアドレスを設定する。相手先アドレスには、当該 SPD 24 のエントリに含まれる設定要求用相手アドレスを設定する。

【0130】

IPsec 設定サーバ 1 からの応答メッセージには設定管理部 26 が送信した

メッセージの ID と要求元アドレス、相手先アドレスが含まれるため、設定管理部 26 はどのメッセージに対する応答なのかを識別することができる。

【0131】

この要求メッセージの一例を図 6 に示す。図 6 に示す例は IPsec 処理装置 2a が IPsec 処理装置 2b との IPsec 通信に必要な設定を要求する要求メッセージの例である。

【0132】

設定管理部 26 は生成した要求メッセージを IPsec 設定サーバ 1 に送信する（図 19 ステップ S43）。設定管理部 26 は IPsec 設定サーバ 1 に要求メッセージを送信すると、5 秒間隔で要求メッセージの送信を繰り返し、IPsec 設定サーバ 1 から要求メッセージに対応する応答を受信するか、要求メッセージを 6 回送信すると、要求メッセージの送信を停止する。

【0133】

設定管理部 26 は 6 回の要求メッセージ送信によって送信を停止した場合や、該当なしエラーメッセージあるいは応答なしエラーメッセージを受信した場合（図 19 ステップ S44, S47）、IPsec 処理部 23 に設定失敗を通知して処理を終了する（図 19 ステップ S49）。

【0134】

尚、設定管理部 26 は要求メッセージの送信を繰り返す場合、常に同じ ID、同じ SPI を使用して送信する。繰り返し送信することによって、1 個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【0135】

設定管理部 26 は IPsec 設定サーバ 1 から内容不一致エラーメッセージを受信した場合（図 19 ステップ S47）、内容不一致エラーメッセージに含まれるエントリ一覧を確認し、エントリ一覧に含まれる ID 及び SPI 以外の値を用いて改めて ID と SPI とを選択し、要求メッセージを IPsec 設定サーバ 1 に送信する（図 19 ステップ S48）。

【0136】

これは I P s e c 処理装置 2 が何らかの原因で動作情報を喪失した後、既に I P s e c 設定サーバ 1 側に登録済みの I D あるいは S P I を使用して要求メッセージを送信した場合である。

【0 1 3 7】

設定管理部 2 6 は内容不一致エラーメッセージで通知された I D や S P I 以外の値を使用することで、I P s e c 設定サーバ 1 の既存の情報と矛盾しない新しい要求メッセージを生成することができる。

【0 1 3 8】

設定管理部 2 6 は I P s e c 設定サーバ 1 から配布メッセージを受信した場合（図 1 9 ステップ S 4 4）、配布メッセージに含まれる適用ポリシーを当該 S P D 2 4 の I P s e c 適用ポリシー欄に設定し、配布メッセージに含まれる S A パラメータを使用して S A を生成し、S A D 2 5 に登録する（図 1 9 ステップ S 4 5）。設定管理部 2 6 は S A を S A D 2 5 に登録したら、I P s e c 処理部 2 3 に設定完了を通知し、処理を終了する（図 1 9 ステップ S 4 6）。

【0 1 3 9】

設定管理部 2 6 は I P s e c 設定サーバ 1 から要求起動メッセージを受信した場合（図 2 0 ステップ S 5 1）、S P D 2 4 のエントリの中から、設定要求用相手アドレスが要求起動メッセージに含まれる相手先アドレスと一致するエントリを検索する（図 2 0 ステップ S 5 2）。一致するエントリが見つからない場合、設定管理部 2 6 は要求起動メッセージを無視する（図 2 0 ステップ S 5 3）。

【0 1 4 0】

この場合、I P s e c 設定サーバ 1 からは 6 回要求起動メッセージが送信されるが、その後、I P s e c 設定サーバ 1 は要求起動メッセージの送信を停止し、元々要求メッセージを送信した I P s e c 処理装置 2 には I P s e c 設定サーバ 1 からエラーメッセージが送信される。

【0 1 4 1】

設定管理部 2 6 は S P D 2 4 の検索によって一致するエントリを見つけた場合、I P s e c 処理部 2 3 から S P D 2 4 のエントリに対する設定取得依頼を受信した時と同様に動作する。すなわち、設定管理部 2 6 は要求メッセージを生成し

て I P s e c 設定サーバ 1 に最大 6 回繰り返し送信する（図 20 ステップ S 5 4 , S 5 5）。

【0142】

但し、I P s e c 処理部 2 3 の依頼による送信ではないので、I P s e c 設定サーバ 1 から配布メッセージやエラーメッセージを受信しても、I P s e c 処理部 2 3 にはその結果を通知しない（図 20 ステップ S 5 6 , S 5 8 , S 6 0）。

【0143】

また、設定管理部 2 3 は要求起動メッセージに対して要求メッセージの送信を開始した場合、繰り返し送信が停止するまで、同一の S P D 2 4 のエントリに対する要求起動メッセージを受信しても新たな要求メッセージの送信を行わない。

【0144】

一方、設定管理部 2 6 は I P s e c 設定サーバ 1 から配布メッセージを受信した場合（図 20 ステップ S 5 6）、配布メッセージに含まれる適用ポリシーを当該 S P D 2 4 の I P s e c 適用ポリシー欄に設定し、配布メッセージに含まれる S A パラメータを使用して S A を生成し、S A D 2 5 に登録する（図 20 ステップ S 5 7）。

【0145】

ルーティング部 2 7 は I P s e c 処理部 2 3 から I P s e c 復号処理済みのデータ通信パケットを受信して、当該パケットが設定管理部 2 6 宛のパケットだった場合、当該パケットを設定管理部 2 6 に転送する。当該パケットが設定管理部 2 6 宛のパケットではない場合、ルーティング部 2 7 は当該パケットを送信すべきインタフェースを決定し、再び I P s e c 処理部 2 3 を介して送信すべきインタフェースに転送する。

【0146】

また、ルーティング部 2 7 は設定管理部 2 6 からのデータ通信パケットを受信し、当該パケットを送信すべきインタフェースを決定して、I P s e c 処理部 2 3 を介して転送する。

【0147】

図 2 1 は図 2 の S P D 1 3 の内容の一例を示す図であり、図 2 2 は図 2 1 に示

す SPD 13 の適用ポリシー (v) の内容を示す図であり、図 23 は従来の IPsec 処理装置の SPD の内容を示す図であり、図 24 は図 23 の SPD の適用ポリシー (j) の内容を示す図である。

【0148】

また、図 25 は図 2 の管理テーブル 17 の IPsec 処理装置 2a から要求メッセージを受信した後の内容を示す図であり、図 26 は図 14 の SPD 24 の設定メッセージを受信して適用ポリシーを設定した後の内容を示す図であり、図 27 は図 2 の管理テーブル 17 の SA を更新するために新しいエントリが生成される場合の内容を示す図であり、図 28 は本発明の一実施例による IPsec 処理装置 2 の動作を示すシーケンスチャートである。

【0149】

これら図 1 ～図 28 を参照して本実施例の IPsec 設定サーバ 1 の具体的な動作について説明する。ここでは図 1 中の IPsec 処理装置 2a に注目し、プライベートネットワーク 201 からプライベートネットワーク 202 宛のデータ通信に対して IPsec 処理装置 2a が IPsec 処理を実施する場合について説明する。まず、IPsec 設定サーバ 1、IPsec 処理装置 2a、IPsec 処理装置 2b に予め必要な設定項目について説明する。

【0150】

IPsec 設定サーバ 1 には IPsec 処理装置 2a 及び IPsec 処理装置 2b との間にそれぞれ安全な IPsec の経路を確保するために、従来と同様の方法で、SPD 13 を設定する。図 21 に示すように、SPD 13 には IPsec 設定サーバ 1 自身から IPsec 処理装置 2a、IPsec 処理装置 2b 宛の通信に対して、それぞれ適用ポリシー (v)、適用ポリシー (w) にしたがって IPsec を適用するように設定している。

【0151】

この適用ポリシー (v) の内容を図 22 に示す。適用ポリシー (v) には IPsec 処理装置 2a との通信を暗号化するためのポリシーが設定されている。また、IPsec 処理装置 2a との間の IPsec 通信において IKE による鍵交換を実施するために、IKE に関するパラメータも設定しておく。

【0152】

尚、本来、IKEに関する設定はIPsec適用ポリシーとは独立に存在するものであるが、説明を容易にするために、本実施例の説明においては適用ポリシーの一部として扱う。適用ポリシー（w）の内容も適用ポリシー（v）と同様の内容である。

【0153】

これらの設定によって、IPsec設定サーバ1とIPsec処理装置2aとの間に安全なIPsecの経路が設定され、設定情報及び秘密鍵の配布を安全に行うことができる。

【0154】

SPD13にはIPsec設定サーバ1と通信するすべてのIPsec処理装置2に対して1件ずつ設定を行う必要がある。例えば、図21に示す例ではIPsec処理装置2a、IPsec処理装置2b以外にもIPsec処理装置2d、IPsec処理装置2eに対するポリシーも設定されている。

【0155】

続いて、IPsec設定サーバ1にはIPsec処理装置2a、IPsec処理装置2b間に適用するIPsecのポリシーを配布ポリシー記憶部16に設定する。配布ポリシー記憶部16の一例を図3に示す。配布ポリシー記憶部16のアドレスペア欄には、IPsec処理装置2a、IPsec処理装置2bのアドレスを、配布ポリシー欄には当該通信に適用するポリシーを設定する。

【0156】

ポリシーでは使用するIPsecプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、SAの有効期間を設定する。また、IPsec設定サーバ1が共有秘密鍵を各IPsec処理装置2a～2fに配布するため、IPsec処理装置2a～2fはIKEを使用しない。したがって、配布ポリシーにはIKEに関するパラメータを設定する必要がない。

【0157】

配布ポリシー記憶部16にはIPsec設定サーバ1が管理する他の通信に対するポリシーをすべて設定しておく。図3に示す例では、IPsec処理装置2

a、IPsec 処理装置 2 b 間の通信以外にも、IPsec 処理装置 2 d、IPsec 処理装置 2 e 間の通信に対するポリシーが設定されている。

【0158】

各 IPsec 処理装置 2 a～2 f には SPD 24 を設定する。SPD 24 には IPsec 設定サーバ 1 との通信を IPsec で暗号化するために通常の IPsec の設定を行い、実際に IPsec を適用したい通信に関しては、セクタ欄と設定要求用相手アドレス欄とを設定する。

【0159】

IPsec 処理装置 2 a の SPD 24 の一例を図 15 に示す。ID=1 のエントリが、IPsec 設定サーバ 1 との通信を暗号化するための設定である。この設定は IPsec 設定サーバ 1 の SPD 13 に設定したものに对应している。適用ポリシー（z）の内容を図 16 に示す。相手先アドレス以外は IPsec 設定サーバ 1 に設定したポリシーと同じであり、IKE に関する設定も含まれる。

【0160】

ID=2 のエントリがプライベートネットワーク 202 宛の通信を暗号化するための設定である。セクタ欄には対象となる通信としてプライベートネットワーク 202 宛の通信を設定し、処理欄には IPsec を設定する。ここで、IPsec 適用ポリシー欄は省略し、設定要求用相手アドレス欄に IPsec 処理装置 2 b のアドレスを設定する。

【0161】

SPD 24 には IPsec 処理装置 2 a が IPsec を適用したい通信をすべて設定する。図 15 に示す例では、IPsec 処理装置 2 b との通信以外にプライベートネットワーク 203 宛の通信に対して IPsec 処理装置 2 c と IPsec 通信を実施する設定となっている。

【0162】

IPsec 処理装置 2 b にも上記と同様の設定を行う。すなわち、SPD 24 に IPsec 設定サーバ 1 用の設定を適用ポリシーとともに設定し、他の IPsec 通信に対してはセクタと設定要求用相手アドレスとを設定しておく。

【0163】

以上が予め必要な設定となる。従来の IPsec 処理装置の SPD に、上記と同様の設定を設定した例を図 23 に示す。従来の IPsec 処理装置では IPsec 設定サーバ 1 用の設定が不要となるが、IPsec を適用するすべての通信について IKE に関する設定を含む適用ポリシーを設定しなければならない。図 23 に示す例では、プライベートネットワーク 202、プライベートネットワーク 203 宛の通信に対してそれぞれ適用ポリシー (j)、適用ポリシー (k) を設定している。適用ポリシー (j) の内容を図 24 に示す。適用ポリシー (j) には IPsec プロトコル、カプセル化モード等の IPsec 適用ポリシーに加えて、IKE のポリシーも設定する。

【0164】

ここで、 n 台の IPsec 処理装置がすべての組み合わせで、互いに IPsec の通信を実施する場合において、本実施例による IPsec 設定サーバ 1 を用いた場合の設定量と従来の IPsec 処理装置に必要な設定量とを比較する。IPsec のポリシーに関する設定と IKE のポリシーに関する設定とをそれぞれ「1」と数えると、従来の IPsec 処理装置では、1 台の IPsec 処理装置に $(n-1)$ 件分の IPsec ポリシーと IKE ポリシーとを設定する必要があるため、1 台当たりの設定量は $2(n-1)$ となり、 n 台で $2n(n-1)$ となる。

【0165】

これに対し、本実施例による IPsec 処理装置 2 では IPsec 設定サーバ 1 との通信用に IPsec ポリシーと IKE ポリシーとを 1 件ずつ設定するのみで、1 台当たりの設定量は 2 となり、 n 台で $2n$ となる。

【0166】

IPsec 設定サーバ 1 には、それぞれの IPsec 処理装置 2 との通信のために IPsec ポリシーと IKE ポリシーとを 1 件ずつ設定することによって $2n$ の設定量と、個々の IPsec 処理装置 2 同士の通信の組合せに対して IPsec ポリシーを 1 件設定するために $n(n-1)/2$ の設定量とが必要となり、IPsec 設定サーバ 1 全体に必要な設定量は $2n + n(n-1)/2$ となる。

【0167】

したがって、本実施例による I P s e c 設定サーバ 1 を用いた場合の設定量は $4n + n(n-1)/2 = n(n+7)/2$ となる。例えば、 $n=10$ の場合には従来の手法の設定量 180 に対して、本発明の設定量が 85 となり、約半分の設定で済むことになる。

【0168】

n^2 の係数に注目すれば、 n が大きくなると、本実施例における設定量が従来の手法の $1/4$ に近づくことがわかり、組合せが多くなるほど効果が大きくなることがわかる。

【0169】

続いて、I P s e c 処理装置 2 a がプライベートネットワーク 202 宛のパケットを受信した後の動作について説明する。I P s e c 処理装置 2 a がプライベートネットワーク 202 宛のパケットをインタフェース部 21 から受信すると、パケットは I P s e c 処理部 23 に渡される。

【0170】

I P s e c 処理部 23 は S P D 24 のセレクトと受信したパケットを比較して該当するエントリを探す。図 15 に示す内容とプライベートネットワーク 202 宛のパケットを比較すると、 $ID=2$ のエントリと一致する。I P s e c 処理部 23 は該当エントリの処理欄にしたがって I P s e c の適用を試みるが、I P s e c 適用ポリシーが設定されておらず、代わりに設定要求用相手アドレスが設定されているため、I P s e c 適用処理を一時中断し、設定管理部 26 に設定の取得を依頼する。

【0171】

設定管理部 26 は I P s e c 処理部 23 から設定取得の依頼を受けると、当該 S P D エントリ用の要求メッセージを生成する。要求メッセージの例を図 6 に示す。ID と S P I とは設定管理部 26 が任意の数値を設定し、要求元アドレスには I P s e c 処理装置 2 a 自身のアドレスを、相手先アドレスには S P D エントリの設定要求用相手アドレスである I P s e c 処理装置 2 b のアドレスを設定する。

【0172】

設定管理部 26 は生成した要求メッセージを IPsec 設定サーバ 1 に送信する。設定管理部 26 は IPsec 設定サーバ 1 に要求メッセージを送信すると、5 秒間隔で要求メッセージの送信を繰り返し、IPsec 設定サーバ 1 から要求メッセージに対応する応答を受信するか要求メッセージを 6 回送信すると要求メッセージの送信を停止する。繰り返し送信することによって、1 個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【0173】

設定管理部 26 から IPsec 設定サーバ 1 に要求メッセージが送信される時、要求メッセージは図 15 に示す SPD 24 の 1 番目のエントリにしたがって、IPsec 処理部 23 によって IPsec を適用されてから IPsec 設定サーバ 1 に送信される。そのため、IPsec 設定サーバ 1 に送信されるメッセージはインターネット 100 上の第 3 者に盗聴されることなく、安全に送信することができる。尚、各 IPsec 処理装置 2 から IPsec 設定サーバ 1 に送信されるメッセージはすべて同様の手順で IPsec を適用されてから送信されるため、以下の説明では IPsec 設定サーバ 1 に送信するメッセージに対して IPsec を適用する手順についてはその説明を省略する。

【0174】

IPsec 設定サーバ 1 に送信された要求メッセージは IPsec 設定サーバ 1 のインタフェース部 11 に到着する。インタフェース部 11 で受信された要求メッセージは IPsec 処理部 12 に送られる。IPsec 処理部 12 では IPsec によって暗号化された要求メッセージを元の状態に復号し、復号後のパケットを要求処理部 15 に送る。

【0175】

尚、各 IPsec 処理装置 2 から IPsec 設定サーバ 1 に送られるメッセージはすべて同様の手順で要求処理部 15 に届くため、以下の説明ではインタフェース部 11 でメッセージが受信されてから要求処理部 15 に届けられるまでの手順についてはその説明を省略する。同様に、IPsec 設定サーバ 1 から IPsec 処理装置 2 に送信されるメッセージに IPsec が適用される手順について

もその説明を省略する。

【0176】

要求処理部15は要求メッセージを受信すると（図12ステップS1）、管理テーブル17からアドレス及びIDが一致するエントリを検索するが、最初は管理テーブル17には何も設定されていないため、一致するエントリが見つからない（図12ステップS2，S7，S9）。

【0177】

要求処理部15は新規登録のため、要求メッセージに含まれる要求元アドレスと相手先アドレスをキーにして配布ポリシー記憶部16の中から該当するエントリを検索する（図13ステップS21）。要求メッセージに含まれる要求元／相手先アドレスはそれぞれIPsec処理装置2a及びIPsec処理装置2bなので、図3に示す配布ポリシー記憶部16の先頭のエントリが一致する。

【0178】

配布ポリシー記憶部16に一致するエントリが見つかったので、要求処理部15は管理テーブル17の新しいエントリを選び、要求元アドレス、相手先アドレス、要求ID、SPI欄にそれぞれ要求メッセージに含まれるIPsec処理装置2aのアドレス、IPsec処理装置2bのアドレス、要求IDの「1001」、SPIの「5100」を設定する。同一エントリのもう一つの要求元アドレス、相手先アドレスにはそれぞれIPsec処理装置2bのアドレス、IPsec処理装置2aのアドレスを設定する。

【0179】

さらに、配布ポリシー記憶部16の該当エントリに設定されている配布ポリシー（a）を管理テーブル17の設定パラメータ欄に設定する（図13ステップS22）。ここまでの設定を終えた管理テーブル17を図25に示す。

【0180】

要求処理部15は相手先アドレスであるIPsec処理装置2bに対して要求起動メッセージを送信する（図13ステップS23）。要求起動メッセージには、相手先アドレスとして要求メッセージの送信元アドレスであるIPsec処理装置2aのアドレスを設定する。要求起動メッセージの一例を図8に示す。

【0 1 8 1】

要求処理部 1 5 は I P s e c 処理装置 2 b から要求メッセージを受信するまで、5 秒間隔で最大 6 回要求起動メッセージを送信する。繰り返し送信することによって、1 個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【0 1 8 2】

I P s e c 処理装置 2 b に送信された要求起動メッセージは I P s e c 処理装置 2 b のインタフェース部 2 2 に到着する。I P s e c 処理装置 2 b では、インタフェース部 2 2 で受信された要求起動メッセージが I P s e c 処理部 2 3 に送られる。

【0 1 8 3】

I P s e c 処理部 2 3 では I P s e c によって暗号化された要求起動メッセージを元の状態に復号し、復号後のパケットをルーティング部 2 7 に送る。ルーティング部 2 7 ではメッセージの宛先が I P s e c 処理装置 2 b 自身であることを判断して、要求起動メッセージを設定管理部 2 6 に渡す。尚、I P s e c 設定サーバ 1 から各 I P s e c 処理装置 2 に送信されるメッセージはすべて同様の手順で設定管理部 2 6 に届くため、以下の説明ではインタフェース部 2 2 でメッセージが受信されてから設定管理部 2 6 に届けられるまでの手順についてはその説明を省略する。

【0 1 8 4】

設定管理部 2 6 は I P s e c 設定サーバ 1 から要求起動メッセージを受信すると、S P D 2 4 のエントリの中から、設定要求用相手アドレスが I P s e c 処理装置 2 a のアドレスと一致するエントリを検索する。I P s e c 処理装置 2 b の S P D 2 4 には予め I P s e c 処理装置 2 a 用のエントリを設定済みであるため、そのエントリと一致する。

【0 1 8 5】

設定管理部 2 6 は当該エントリのポリシーを取得するために要求メッセージを生成する。要求メッセージでは要求元アドレス、相手先アドレスにそれぞれ I P s e c 処理装置 2 b、I P s e c 処理装置 2 a のアドレスを設定し、I D 及び S

PIにはそれぞれ設定管理部26が任意に選択した要求ID「2001」、SPI「6100」を設定する。

【0186】

設定管理部26は生成した要求メッセージをIPsec設定サーバ1に送信する。設定管理部26はIPsec設定サーバ1に要求メッセージを送信すると、5秒間隔で要求メッセージの送信を繰り返し、IPsec設定サーバ1から要求メッセージに対応する応答を受信するか、要求メッセージを6回送信すると、要求メッセージの送信を停止する。

【0187】

IPsec処理装置2bから送信された要求メッセージはIPsec設定サーバ1のインタフェース部11に到着し、要求処理部15に転送される。要求処理部15はIPsec処理装置2bから要求メッセージを受信すると、要求起動メッセージの送信を停止し、要求メッセージの受信処理（図12ステップS1）を開始する。

【0188】

要求処理部15は図25に示す管理テーブル17から要求メッセージに含まれるアドレス及びIDが一致するエントリを検索するが、IDが一致するエントリは存在しない（図12ステップS2）。また、アドレス及びSPIが一致するエントリも存在しない（図12ステップS7）。

【0189】

続いて、要求処理部15は管理テーブル17においてアドレスが一致してIDが空欄のエントリを検索する（図12ステップS9）。図25に示す最初のエントリが該当するので、要求処理部15は要求メッセージに含まれる値を使用して、空欄になっているID欄及びSPI欄に要求ID「2001」、SPI「6100」をそれぞれ設定する。

【0190】

さらに、IPsec処理装置2aからIPsec処理装置2bへの順方向用のSAパラメータと、逆方向用のSAパラメータとを生成する（図12ステップS10）。具体的には、IPsecプロトコル、カプセル化モード、暗号化アルゴ

リズム、認証アルゴリズム、有効期限について配布ポリシー（a）と同一の内容を設定し、暗号化鍵、認証鍵、I Vについては乱数生成器 18 から乱数を取得して値を設定する。

【0191】

また、受信側 S P I 欄には受信側となる I P s e c 処理装置 2 が使用する S P I を設定する。設定後の管理テーブル 17 の内容を図 4 に示す。1 番目のエントリについて、要求 I D の欄に「2001」が設定され、S P I の欄に「6100」が設定され、それぞれの方向用の S A パラメータには S A パラメータ（a）と S A パラメータ（b）とが設定されている。S A パラメータ（a）の内容を図 5 に示す。逆方向の S A パラメータ（b）では暗号化鍵、認証鍵、I V として異なる乱数値が使用されることと、受信側 S P I の値が I P s e c 処理装置 2 a 用の「5100」となること以外は同じ内容となる。

【0192】

要求処理部 15 は管理テーブル 17 の設定パラメータ欄の内容を使用して配布メッセージを作成し、I P s e c 処理装置 2 a と I P s e c 処理装置 2 b に対してそれぞれ送信する（図 12 ステップ S 11）。

【0193】

この時、送信する配布メッセージに設定する要求元アドレス、相手先アドレス、I D は管理テーブル 17 の当該エントリで示される値を使用する。したがって、I P s e c 処理装置 2 a 宛の配布メッセージでは要求元アドレス、相手先アドレス、I D の値はそれぞれ I P s e c 処理装置 2 a のアドレス、I P s e c 処理装置 2 b のアドレス、要求 I D 「1001」となり、I P s e c 処理装置 2 b 宛の配布メッセージではそれぞれ I P s e c 処理装置 2 b のアドレス、I P s e c 処理装置 2 a のアドレス、要求 I D 「2001」となる。I P s e c 処理装置 2 a 宛の配布メッセージの内容を図 7 に示す。

【0194】

要求処理部 15 は配布メッセージを送信後、タイマ 19 を使用して S A パラメータの有効期限と同じ時間を計測し、タイマ 19 が満了した時点で管理テーブル 17 の当該エントリを削除する。

【0195】

IPsec 設定サーバ 1 から IPsec 処理装置 2 a に送信された配布メッセージは IPsec 処理装置 2 a のインタフェース部 2 2 に到着し、設定管理部 2 6 に転送される。

【0196】

IPsec 処理装置 2 a の設定管理部 2 6 は IPsec 設定サーバ 1 から配布メッセージを受信すると、要求メッセージの送信を停止し、配布メッセージに含まれる適用ポリシーを SPD 2 4 の IPsec 適用ポリシー欄に設定する。ポリシーを設定した後の SPD 2 4 の内容を図 2 6 に示す。

【0197】

さらに、設定管理部 2 6 は配布メッセージに含まれる SA パラメータを使用して、双方向の通信用にそれぞれ SA を生成し、SAD 2 5 に設定する。IPsec 処理装置 2 a から IPsec 処理装置 2 b 方向の SA を設定した SAD 2 5 の内容を図 1 7 に示す。

【0198】

SAD 2 5 の 1 番目のエントリが該当エントリである。配布メッセージで通知された SA パラメータ (a) はシーケンス番号が加えられて SAD 2 5 に設定されている。受信用の SAD 2 5 も配布メッセージによって通知された SA パラメータ (b) の内容にしたがって同様に設定する。この時点で IPsec 処理装置 2 a の IPsec 処理部 2 3 が IPsec 処理装置 2 b 宛の通信に対する IPsec の処理を実施できるようになる。

【0199】

設定管理部 2 6 は SPD 2 4 及び SAD 2 5 の設定を終えると、IPsec 処理部 2 3 に設定完了を通知する。IPsec 処理部 2 3 は設定管理部 2 6 から設定完了通知を受信すると、一時中断していたデータ通信パケットの処理を再開する。この時点では、SPD 2 4 のエントリの適用ポリシー及び対応する SAD 2 5 のエントリが存在するため、IPsec 処理部 2 3 は従来通りの IPsec 処理を実施することができる。

【0200】

IPsecを適用されたパケットはIPsec処理装置2b宛に送信される。IPsec処理装置2b側もIPsec設定サーバ1から配布メッセージを受信した時点でSPD24及びSAD25にエントリを設定しているため、IPsec処理装置2aからIPsec適用済みパケットを受信した時点で従来の手順でIPsecの復号処理を実施することができる。

【0201】

IPsec処理装置2bのIPsec処理部23によって復号処理されたパケットは、インタフェース部21からプライベートネットワーク202に送出される。このようにして、プライベートネットワーク201から送出されたパケットはプライベートネットワーク202に到達する。

【0202】

この時、さらにプライベートネットワーク201からプライベートネットワーク202宛のパケットが引き続き発生した場合について説明する。IPsec処理装置2aのIPsec処理部23は図26に示すSPD24を検索し、2番目のエントリにすでにポリシーが存在することを確認し、さらに図17に示すSAD25を検索して1番目のエントリに当該SAが存在することも確認し、当該SAを使用してIPsecの処理を実施する。すなわち、IPsec設定サーバ1から設定パラメータを取得した後は、従来のIPsecと同様に動作する。

【0203】

続いて、SA更新時の動作について説明する。IPsec処理装置2aのIPsec処理部23はSAD25を監視し、有効期限が満了するエントリについてSAの更新を実施する。

【0204】

SAを更新する場合、IPsec処理部23は設定管理部26に設定取得を依頼する。この時、IPsec処理部23は当該SAに対応するSPD24のエントリを設定管理部26に通知する。

【0205】

設定管理部26はIPsec処理部23から設定取得の依頼を受けると、当該SPDエントリ用の要求メッセージを生成する。要求メッセージではID及びS

P I 以外は最初に送信した要求メッセージと同一の内容を設定する。I D 及び S P I は新しい値を設定する。ここでは設定管理部 26 が I D 及び S P I の値としてそれぞれ「1002」, 「5110」を選択したものとする。

【0206】

設定管理部 26 は生成した要求メッセージを I P s e c 設定サーバ 1 に送信する。設定管理部 26 は I P s e c 設定サーバ 1 に要求メッセージを送信すると、5 秒間隔で要求メッセージの送信を繰り返し、I P s e c 設定サーバ 1 から要求メッセージに対応する応答を受信するか、要求メッセージを 6 回送信すると、要求メッセージの送信を停止する。

【0207】

I P s e c 設定サーバ 1 に送信された要求メッセージは I P s e c 設定サーバ 1 のインタフェース部 11 に到着し、要求処理部 15 に届けられる。要求処理部 15 は要求メッセージを受信すると（図 12 ステップ S1）、管理テーブル 17 からアドレス及び I D が一致するエントリを検索するが、I D 及び S P I がともに新しい値のため、一致するエントリが見つからない（図 12 ステップ S2, S7）。また、この時点では I D が空欄のエントリも存在しない（図 12 ステップ S9）。

【0208】

これ以降は初めて要求メッセージを受信した時の動作と同じ手順となる。すなわち、要求処理部 15 は配布ポリシー記憶部 16 を検索し（図 13 ステップ S21）、管理テーブル 17 に新しくエントリを登録する（図 13 ステップ S22）。この時点での管理テーブル 17 の内容を図 4 に示す。I D 及び S P I 欄がそれぞれ「1002」, 「5110」であるエントリが 2 番目に追加されていることがわかる。

【0209】

要求処理部 15 は相手先となる I P s e c 処理装置 2 b に要求起動メッセージを送信する（図 13 ステップ S23）。I P s e c 処理装置 2 b では要求起動メッセージを受信すると、やはり新しい I D と S P I とを設定して要求メッセージを送信する。ここでは、I P s e c 処理装置 2 b が新しい I D、S P I としてそ

れぞれ「2002」, 「6110」を選択したものとする。

【0210】

IPsec 設定サーバ 1 の要求処理部 15 は IPsec 処理装置 2 b から要求メッセージを受信すると (図 12 ステップ S1)、アドレスは一致するが、ID が空欄のエントリを発見し (図 12 ステップ S9)、要求メッセージで通知された ID 及び SPI と、生成した SA パラメータとを管理テーブル 17 に設定する (図 12 ステップ S10)。この時点での管理テーブル 17 の内容を図 27 に示す。

【0211】

図 27 に示す内容を図 4 に示す内容と比較すると、空欄だった ID, SPI 欄に「2002」, 「6110」が設定され、SA パラメータも設定されていることがわかる。さらに、要求処理部 15 は管理テーブル 17 の内容にしたがって配布メッセージを生成し、IPsec 処理装置 2 a 及び IPsec 処理装置 2 b に対してそれぞれ送信する (図 12 ステップ S11)。

【0212】

各 IPsec 処理装置 2 の設定管理部 26 は配布メッセージを受信すると、配布メッセージで通知されたポリシーを SPD 24 に設定し、通知された SA パラメータから SA を生成して SAD 25 を設定する。この時点で、新しい SA が利用可能となり、SA の更新が完了する。

【0213】

ここで、IPsec 処理装置 2 がインタフェース部 21 から IPsec を適用する最初のパケットを受信した後、実際に IPsec 処理を実施してパケットをインタフェース部 22 に送信するまでの処理について、従来の IPsec による手順と本実施例による手順とを比較する。

【0214】

従来の手法では、図 32 に示すように、インタフェース部 41 からパケットを受信すると、IPsec 処理部 43 が IKE による公開鍵の演算を実施し、通信相手となる IPsec 処理装置と公開鍵を交換する。IPsec 処理部 43 はさらに秘密鍵の演算を実施し、得られた秘密鍵を用いて IPsec を適用し、パケ

ットをインタフェース部 42 に送る。

【0215】

これに対し、本実施例の手順では、図 28 に示すように、IPsec 処理部 23 がインタフェース部 21 からパケットを受信すると、IPsec 処理部 23 は設定管理部 26 に設定取得を依頼し、設定管理部 26 は IPsec 設定サーバ 1 に要求メッセージを送信する。

【0216】

設定管理部 26 は IPsec 設定サーバ 1 から配布メッセージを受信すると、IPsec 処理部 23 に設定完了を通知し、IPsec 処理部 23 はパケットに IPsec を適用してインタフェース部 22 に送る。

【0217】

インタフェース部 21 がパケットを受信してから IPsec 処理を実施してパケットをインタフェース部 22 に送信するまでの時間を、従来の手順、本実施例の手順についてそれぞれ T_b 、 T_a とする。この時、従来の手順では公開鍵及び秘密鍵の演算に時間がかかるため、 $T_b > T_a$ となり、本実施例の手順の方が早くパケットを転送できることがわかる。

【0218】

例えば、IKE の Diffie-Hellman 鍵共有アルゴリズムで使用するグループを 1536 ビット MODP (Modular Exponentiation Group) として 50MHz の RISC (Reduced Instruction Set Computer) プロセッサを使用した場合、 T_b は約 18 秒 (実測値) となるが、 T_a は 1 秒未満となる。

【0219】

厳密には、本実施例の手順の要求メッセージは従来の IPsec の手順で送信されるため、この時、IKE の鍵交換が実施される場合には $T_b < T_a$ となるが、それ以降の IPsec 通信については相手先となる IPsec 処理装置 2 の組合せに関係なく、IPsec 設定サーバ 1 用の IKE の SA が有効な間は $T_b > T_a$ となる。

【0220】

また、従来の手法においてIKEの公開鍵あるいは秘密鍵の演算を実施する場合には、IPsec処理装置がIKEの演算処理に集中してしまうため、IPsecを適用する必要のないパケットの転送速度が低下してしまう。IKEの鍵交換処理は通信している相手毎に定期的に発生するため、IPsec通信をする相手が多いほど処理能力が低下する割合が大きくなる。

【0221】

それに対して本実施例の手順では、IPsec処理装置2とIPsec設定サーバ1との間で定期的に鍵交換処理が発生するが、通信相手となる各IPsec処理装置2に対しては鍵交換処理を行わないため、IPsec通信をする相手が増えたとしても処理能力が低下する割合は一定である。

【0222】

例えば、IKEのDiffie-Hellman鍵共有アルゴリズムで使用するグループを1536ビットMODP、IKEのSAの有効期限を1時間として50MHzのRISCプロセッサを使用した場合、IPsec処理装置が他の10台のIPsec処理装置との間でIPsec通信を実施すると、従来の手順では1時間の間にIKEの鍵交換が10回ずつ実施されることになり、1時間当たり約180秒間性能が低下することになる。

【0223】

それに対して、本実施例の手法では、IPsec設定サーバ1との間でIKEの鍵交換が実施されるのみなので、1時間当たり約18秒間の性能低下のみとなる。

【0224】

IKEの演算処理速度に起因する問題を解決する既存の手段として、演算専用回路をIPsec処理装置に搭載し、IKEの演算処理自体を高速化する方法がある。演算専用回路を搭載したIPsec処理装置の例を図33に示す。演算専用回路51がIPsec処理部43に接続されている点が、図31に示す従来のIPsec処理装置4と異なる。

【0225】

IPsec処理部43はIKEの演算が必要になると、演算専用回路51に演

算を依頼する。演算専用回路 51 によって高速に演算が実施されるため、図 32 に示す従来手法の演算処理に要する時間が短くなり、全体の速度も向上する。この手段を用いれば、IKE の演算速度に起因する問題を解決することが可能である。但し、演算専用回路 51 を持たない IPsec 処理装置をすでに導入してしまっている場合には、IPsec 処理装置そのものを演算専用回路付きの IPsec 処理装置に置き換える必要がある。

【0226】

それに対して、本実施例の方法では必要となる機能をすべてソフトウェアで実現することができるため、すでに導入済みの IPsec 処理装置に対してもソフトウェアのバージョンアップで機能を追加することが可能であり、既存の設備を有効活用することができる。

【0227】

このように、本実施例では使用するサービスやアルゴリズム等の情報を IPsec 設定サーバ 1 に一括して設定することによって、IPsec 処理装置 2, 2a~2f がほとんどの設定を IPsec 設定サーバ 1 から取得することが可能となるため、IPsec 処理装置 2, 2a~2f への設定を少なくすることができる。

【0228】

また、本実施例では、IPsec 処理装置 2, 2a~2f において IKE を使用せずに、秘密鍵を更新することによって、IKE に関する設定が不要となるので、IPsec 処理装置 2, 2a~2f への設定を少なくすることができる。

【0229】

さらに、本実施例では、IPsec 設定サーバ 1 を用いることによって、従来、IPsec を実施する両端の装置にそれぞれ同一の設定を行う必要があるが、IPsec 設定サーバ 1 がそれぞれの装置に設定していた内容を自装置のみに設定すればよいため、IPsec 処理に関する設定の総数を少なくすることができる。

【0230】

上記のほかに、本実施例では、要求起動メッセージを送信しているので、要求

メッセージの送信元の I P s e c 処理装置に対向する I P s e c 処理装置ではその送信元の I P s e c 処理装置での I P s e c のポリシーの設定とはほぼ同時に I P s e c のポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元の I P s e c 処理装置がパケットを暗号化して送信すると、対向する I P s e c 処理装置では送信元の I P s e c 処理装置からのパケットを復号して受取ることができる。

【0231】

これによって、本実施例では、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信先の I P s e c 処理装置において送信元からのパケットを取りこぼしなく受取ることができ、対向する I P s e c 処理装置で送信元からのパケットを復号するまでの時間を大幅に短縮することができる。

【0232】

また、本実施例では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向する I P s e c 処理装置から送られてこなければ、送信元の I P s e c 処理装置に対して応答なしエラーメッセージが送信されるので、送信元の I P s e c 処理装置で対向装置の不存在を即座に認識することができる。

【0233】

上記と同様に、本実施例では、I P s e c 設定サーバ1を用いることによって、従来、I P s e c を実施する両端の装置に同一の設定をそれぞれ個別に設定する必要があるので、設定内容の不一致が発生する可能性があるが、I P s e c 設定サーバ1が両端の装置に同一の設定を配信し、設定内容の不一致が発生しなくなるため、I P s e c の設定不一致による接続障害がなくなる。

【0234】

また、本実施例では、従来、定期的に共有秘密鍵を更新するために I K E を使用した複雑な演算が必要であるが、I K E の代わりに I P s e c 設定サーバ1から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、I K E を使用した場合と比較して通信を開始できるまでの時間が短くなる。

【0235】

これと同様に、本実施例では、従来、定期的に共有秘密鍵を更新するためにIKEを使用した複雑な演算が必要であるが、IKEの代わりにIPsec設定サーバ1から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、IKEを使用した場合と比較してIPsec処理を実施する装置の演算負荷を軽減することができる。

【0236】

図29は本発明の他の実施例によるIPsec処理装置の構成を示すブロック図である。図29においては、IPsec処理装置3がルータではなく、パーソナルコンピュータの場合の適用例を示している。

【0237】

本発明の他の実施例によるIPsec処理装置3はインタフェース部21を省き、上位アプリケーション部31を設けた以外は図14に示す本発明の一実施例によるIPsec処理装置2と同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。

【0238】

上位アプリケーション部31はデータ通信パケットを送受信する実体であり、ルーティング部27に接続されている。ルーティング部27は送受信されるパケットが上位アプリケーション部31宛なのか、設定管理部26宛なのか、あるいはインターネット100宛なのかを判断してパケットをそれぞれの宛先に転送する。

【0239】

ここで、図1におけるIPsec処理装置2dとIPsec処理装置2eとがパーソナルコンピュータであるものとし、IPsec処理装置2dからIPsec処理装置2eに対してパケットを送信する場合について考える。

【0240】

ルータの場合と同様に、IPsec設定サーバ1にはIPsec処理装置2d、IPsec処理装置2eとの間にそれぞれ安全なIPsecの経路を確保するためにSPD13を設定し、IPsec処理装置2d、IPsec処理装置2e

間に適用する I P s e c のポリシーを配布ポリシー記憶部 16 に設定する。

【0241】

これら I P s e c 処理装置 2 d, 2 e には S P D 2 4 を設定する。I P s e c 設定サーバ 1 との通信を暗号化するために通常の I P s e c の設定を行い、実際に I P s e c を適用したい通信に関しては、セクタと設定要求用相手アドレスとを設定する。

【0242】

I P s e c 処理装置 2 d からパケットが送信される場合、パケットを送受信する実体である上位アプリケーション部 31 からデータ通信パケットがルーティング部 27 に渡される。ルーティング部 27 ではパケットの宛先がインターネット側であることを認識して、パケットを I P s e c 処理部 23 に転送する。

【0243】

これ以降は、ルータの場合の実施例と同じである。すなわち、I P s e c 処理部 23 は S P D 2 4 のセクタとパケットとを比較して該当するエントリを検索し、該当するエントリに示された処理が I P s e c であれば、I P s e c の適用を実施する。

【0244】

この時、該当するエントリに I P s e c 適用のポリシーが存在しない場合、I P s e c 処理部 23 はパケットの処理を一時中断し、設定管理部 26 に設定要求を依頼する。設定管理部 26 は I P s e c 設定サーバ 1 に要求メッセージを送信し、配布メッセージを受信することで S P D 2 4 と S A D 2 5 とを設定し、I P s e c 処理部 23 に設定完了を通知する。I P s e c 処理部 23 は中断していたパケットの処理を再開し、設定された S A を使用して I P s e c を適用したうえで、パケットをインタフェース部 22 経由でインターネット 100 に転送する。

【0245】

受信時もルータの場合とほぼ同様である。I P s e c 処理装置 2 d, 2 e ではすでに設定管理部 26 によって S P D 2 4、S A D 2 5 が設定されている。インタフェース部 22 経由で受信した I P s e c 適用済みパケットは I P s e c 処理部 23 に転送される。I P s e c 処理部 23 は S A D 2 5 から該当する S A を検

索し、パケットの復号処理を行う。

【0246】

復号処理によって元の状態に戻ったパケットはルーティング部 27 に転送される。ルーティング部 27 ではパケットが上位アプリケーション部 31 宛であるか、設定管理部 26 宛であるかを判断し、上位アプリケーション部 31 宛であれば上位アプリケーション部 31 に転送する。

【0247】

このようにすることで、パケットの受信処理が完了する。したがって、本実施例では IPsec 処理装置 2d, 2e がルータの場合でもパーソナルコンピュータの場合でも適用することができる。

【0248】

図 30 は本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。本発明の一実施例では IPsec 設定サーバ 1 の配布ポリシー記憶部 10 に、実際に IPsec 通信を行う IPsec 処理装置 2 間に適用するポリシーを個々の通信毎に設定する必要があるが、本発明の別の実施例ではいくつかの組合せについて共通のポリシーを利用することで、配布ポリシー記憶部 16 に設定するポリシーの数を減らしている。尚、本発明の別の実施例による IPsec 設定サーバの構成は図 2 に示す本発明の一実施例による IPsec 設定サーバ 1 の構成と同様になっている。

【0249】

本実施例において、配布ポリシー記憶部 16 は特定のアドレスの組合せに対してポリシーを設定すると同時に、任意の組合せにおけるポリシーを設定することが可能となっている。図 30 に示す例では、IPsec 処理装置 2d、IPsec 処理装置 2e 間の通信に適用するポリシーと、それ以外のすべての組合せに適用するポリシーとが設定されている。本実施例の場合、多くの IPsec 処理装置 2 が共通のポリシーを利用することで、配布ポリシー記憶部 16 に設定するポリシーの数を減らすことができる。

【0250】

ここで、n 台の IPsec 処理装置がすべての組合せで、互いに IPsec の

通信を実施する場合において、本実施例に必要な設定量と従来の I P s e c 処理装置に必要な設定量とを比較する。この時、すべての I P s e c 通信の組合せにおいて同一のポリシーを適用することとする。

【0251】

従来の I P s e c 処理装置に必要な設定量の合計は先に計算した通り、 $2n(n-1)$ である。それに対し、本実施例においては、I P s e c 処理装置同士の通信の組合せの数に関わらず、I P s e c ポリシーの設定量は 1 件だけでよい。したがって、本実施例において必要となる設定量は $4n+1$ となる。

【0252】

これからわかる通り、従来の手法では設定量が n の 2 乗に比例して多くなるが、本実施例では設定量が n に比例して大きくなるため、組合せが多くなるほど効果が大きくなることがわかる。例えば、 $n=10$ の場合には、従来の手法の設定量が 180 に対して、本実施例の設定量が 41 となり、約 $1/4$ の設定で済むことがわかる。

【0253】

【発明の効果】

以上説明したように本発明の装置及び方法は、I P s e c 処理装置間に適用する I P s e c のポリシーを一括管理することによって、通信する装置間での設定不一致を防止することができるという効果が得られる。

【0254】

また、本発明の他の装置及び方法は、要求メッセージを受信した場合に当該要求メッセージを送信した I P s e c 処理装置の通信相手である I P s e c 処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるという効果が得られる。

【0255】

さらに、本発明の別の装置及び方法は、I P s e c の暗号化や認証に使用するための共有秘密鍵を生成し、その生成した共有秘密鍵を I P s e c 処理装置に配

布することによって、共有秘密鍵演算を不要とし、個々の装置での通信開始時の I P s e c 経路の接続時間を短縮することができ、性能の低下を防ぐことができるという効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の一実施例による I P s e c によるネットワークの構成を示すブロック図である。

【図 2】

図 1 の I P s e c 設定サーバの構成を示すブロック図である。

【図 3】

図 2 の配布ポリシー記憶部の記憶内容を示す図である。

【図 4】

図 2 の管理テーブルの記憶内容を示す図である。

【図 5】

図 4 の S A パラメータの内容を示す図である。

【図 6】

本発明の一実施例による要求メッセージの一例を示す図である。

【図 7】

本発明の一実施例による配布メッセージの一例を示す図である。

【図 8】

本発明の一実施例による要求起動メッセージの一例を示す図である。

【図 9】

本発明の一実施例による該当なしエラーメッセージの一例を示す図である。

【図 1 0】

本発明の一実施例による内容不一致エラーメッセージの一例を示す図である。

【図 1 1】

本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【図 1 2】

本発明の一実施例による I P s e c 設定サーバの動作を示すフローチャートで

ある。

【図 1 3】

本発明の一実施例による I P s e c 設定サーバの動作を示すフローチャートである。

【図 1 4】

図 1 の I P s e c 処理装置の構成を示すブロック図である。

【図 1 5】

図 1 4 の S P D の内容を示す図である。

【図 1 6】

図 1 5 に示す S P D の適用ポリシー（z）の一例を示す図である。

【図 1 7】

図 1 4 の S A D の内容を示す図である。

【図 1 8】

図 1 4 の I P s e c 処理部の処理動作を示すフローチャートである。

【図 1 9】

図 1 4 の設定管理部の処理動作を示すフローチャートである。

【図 2 0】

図 1 4 の設定管理部の処理動作を示すフローチャートである。

【図 2 1】

図 2 の S P D の内容の一例を示す図である。

【図 2 2】

図 2 1 に示す S P D の適用ポリシー（v）の内容を示す図である。

【図 2 3】

従来の I P s e c 処理装置の S P D の内容を示す図である。

【図 2 4】

図 2 3 の S P D の適用ポリシー（j）の内容を示す図である。

【図 2 5】

図 2 の管理テーブルの I P s e c 処理装置から要求メッセージを受信した後の内容を示す図である。

【図 2 6】

図 1 4 の S P D の配布メッセージを受信して適用ポリシーを設定した後の内容を示す図である。

【図 2 7】

図 2 の管理テーブルの S A を更新するために新しいエントリが生成される場合の内容を示す図である。

【図 2 8】

本発明の一実施例による I P s e c 処理装置の動作を示すシーケンスチャートである。

【図 2 9】

本発明の他の実施例による I P s e c 処理装置の構成を示すブロック図である。

【図 3 0】

本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。

【図 3 1】

従来の I P s e c 処理装置の構成を示すブロック図である。

【図 3 2】

従来の I P s e c 処理装置の動作を示すシーケンスチャートである。

【図 3 3】

従来の I P s e c 処理装置の他の構成を示すブロック図である。

【符号の説明】

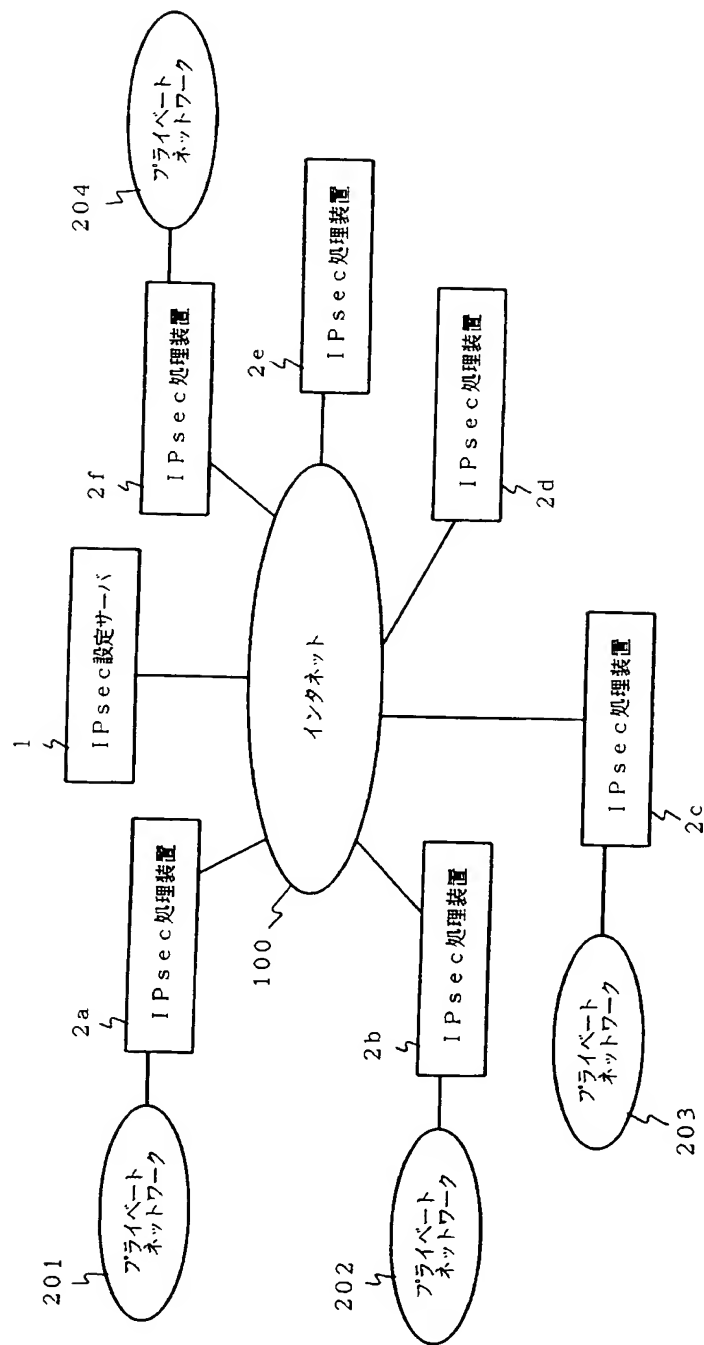
- 1 I P s e c 設定サーバ
- 2, 2 a ~ 2 f, 3 I P s e c 処理装置
- 1 1, 2 1, 2 2 インタフェース部
- 1 2, 2 3 I P s e c 処理部
- 1 3, 2 4 S P D
- 1 4, 2 5 S A D
- 1 5 要求処理部
- 1 6 配布ポリシー記憶部

- 1 7 管理テーブル
- 1 8 乱数生成器
- 1 9 タイマ
- 2 0, 2 8 記録媒体
- 2 6 設定管理部
- 2 7 ルーティング部
- 3 1 上位アプリケーション部
- 1 0 0 インタネット
- 2 0 1 ~ 2 0 4 プライベートネットワーク

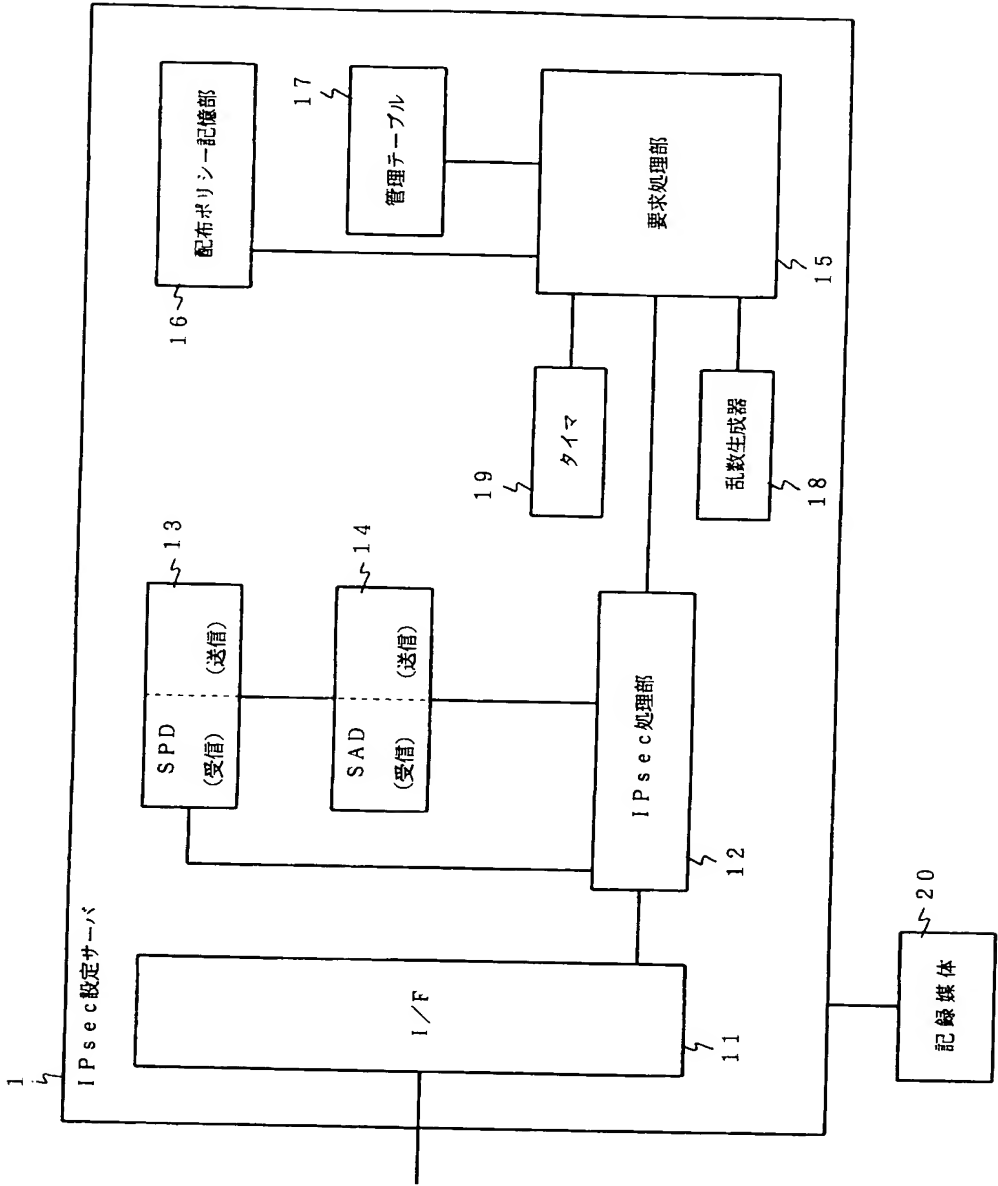
【書類名】

図面

【図 1】



【図 2】



【図 3】

アドレスペア		配布ポリシー	配布ポリシー (a)	配布ポリシー (b)
IPsec 処理装置 2a	IPsec 処理装置 2b	IPsec プロトコル カプセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間		
		ESP トンネルモード DES-CBC HMAC-MD5-96 3600秒		
IPsec 処理装置 2d	IPsec 処理装置 2e	IPsec プロトコル カプセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間		
		ESP トランスポートモード 3DES-CBC HMAC-SHA-1-96 3600秒		

【図 4】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置 2a	IPsec 処理装置 2b	1001	5100	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー (a) SAパラメータ (a) SAパラメータ (b)
	IPsec 処理装置 2b	IPsec 処理装置 2a	2001	6100	
2	IPsec 処理装置 2a	IPsec 処理装置 2b	1002	5110	適用ポリシー 2a→2b用SAパラメータ 2b→2a用SAパラメータ 配布ポリシー (a)
	IPsec 処理装置 2b	IPsec 処理装置 2a			
3					

【図 5】

I P s e c プロトコル	E S P
カプセル化モード	トンネルモード
暗号化アルゴリズム	D E S - C B C
認証アルゴリズム	H M A C - M D 5 - 9 6
有効期限	3 6 0 0 秒
暗号化鍵	0 x 7 d 5 e 8 3 7 a d . . .
認証鍵	0 x 8 9 e 5 6 2 b f c . . .
I V	0 x c 3 2 f b e 0 0 4 . . .
受信側 S P I	6 1 0 0

【図 6】

メッセージタイプ	要求メッセージ
I D	1 0 0 1
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b
S P I	5 1 0 0

【図 7】

メッセージタイプ	配布メッセージ
I D	1 0 0 1
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b
設定パラメータ	
運用ポリシー	配布ポリシー (a)
2 a → 2 b 用 S A パラメータ	S A パラメータ (a)
2 b → 2 a 用 S A パラメータ	S A パラメータ (b)

【図 8】

メッセージタイプ	要求起動メッセージ
相手先アドレス	I P s e c 処理装置 2 a

【図 9】

メッセージタイプ	該当なしエラーメッセージ
I D	1 0 0 1
要求元アドレス	I P s e c 処理装置 2 a
相手先アドレス	I P s e c 処理装置 2 b

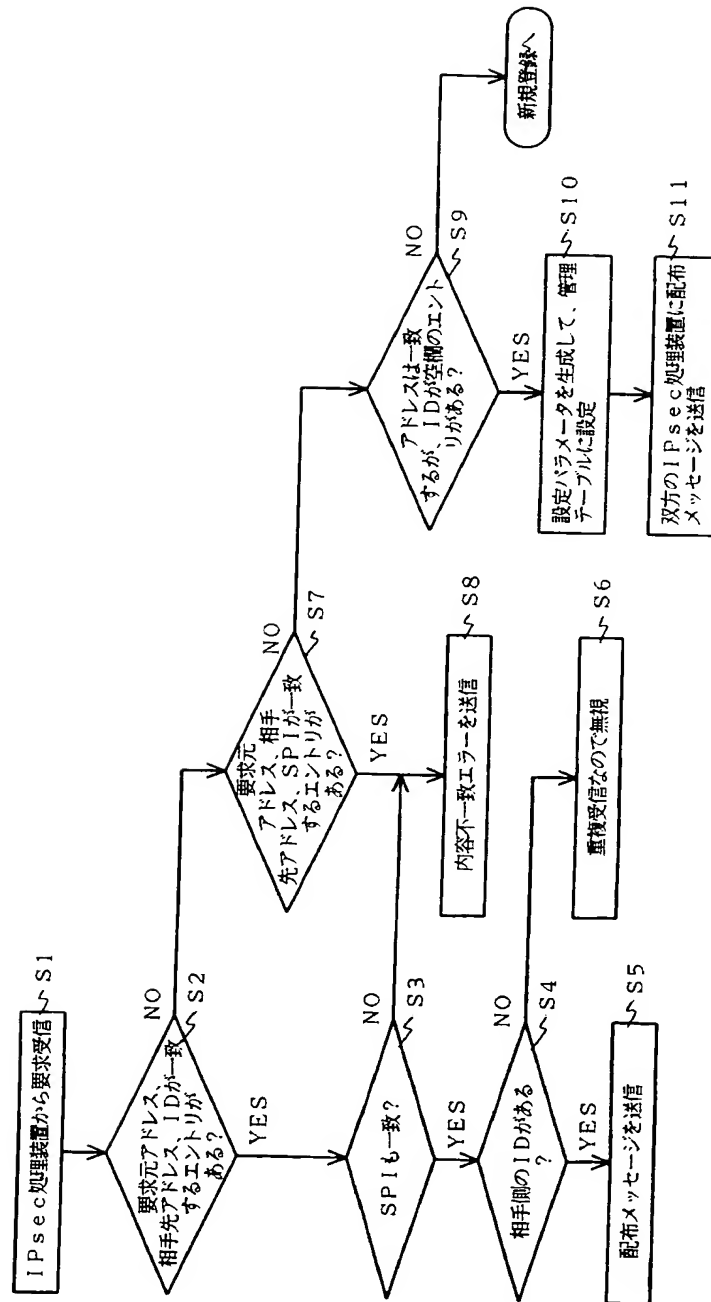
【図 10】

メッセージタイプ	内容不一致エラーメッセージ	
ID	1001	
要求元アドレス	IPsec処理装置2a	
相手先アドレス	IPsec処理装置2b	
エントリ一覧	ID	SPI
	1001	5100
	1002	5110

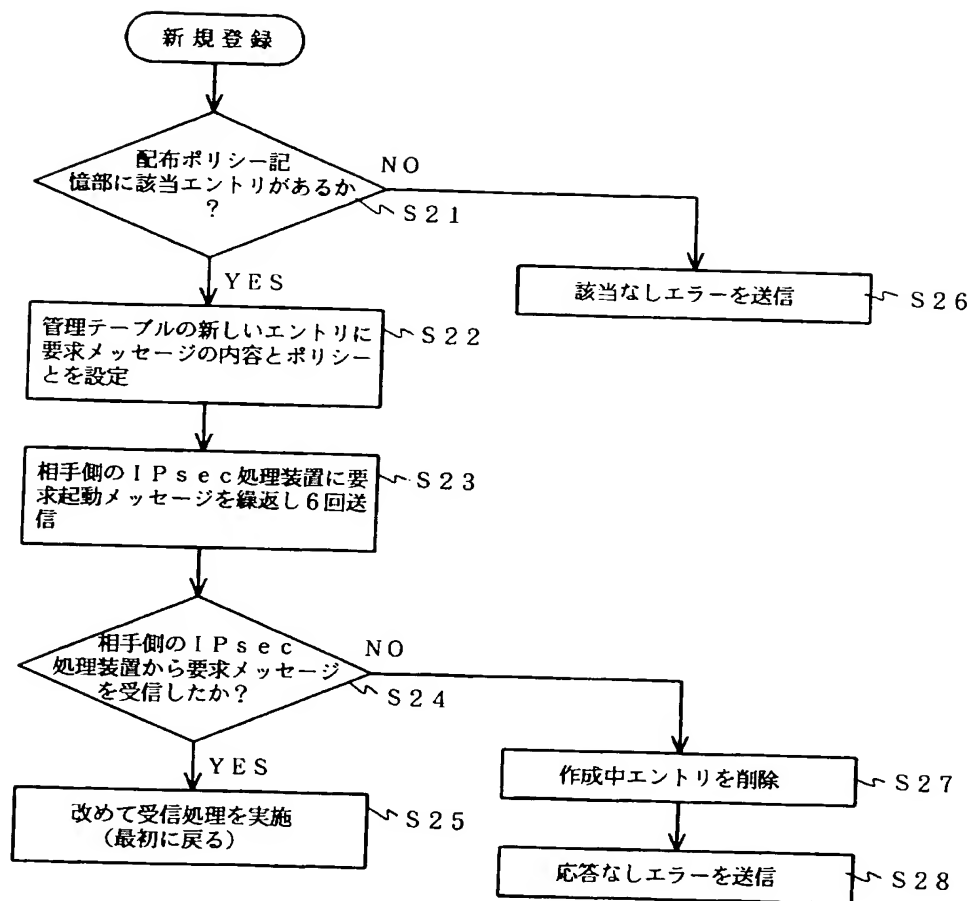
【図 11】

メッセージタイプ	応答なしエラーメッセージ
ID	1001
要求元アドレス	IPsec処理装置2a
相手先アドレス	IPsec処理装置2b

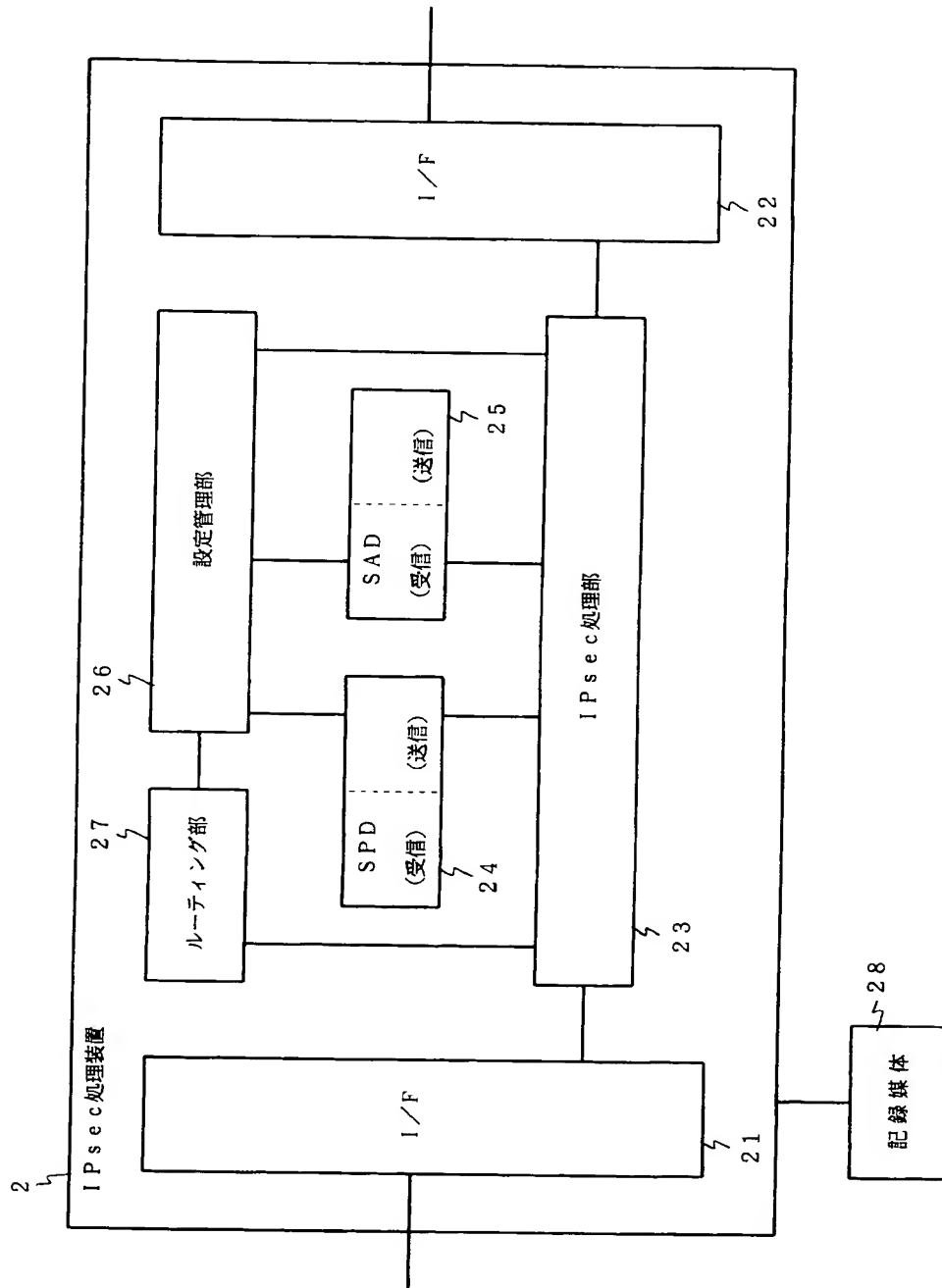
【図 12】



【図13】



【図 14】



【図 15】

ID	セクタ	処理	IPsec適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ1	IPsec	適用ポリシー (z)	
2	プライベート202宛	IPsec		IPsec処理装置2b
3	プライベート203宛	IPsec		IPsec処理装置2c
4	上記以外すべて	通過		

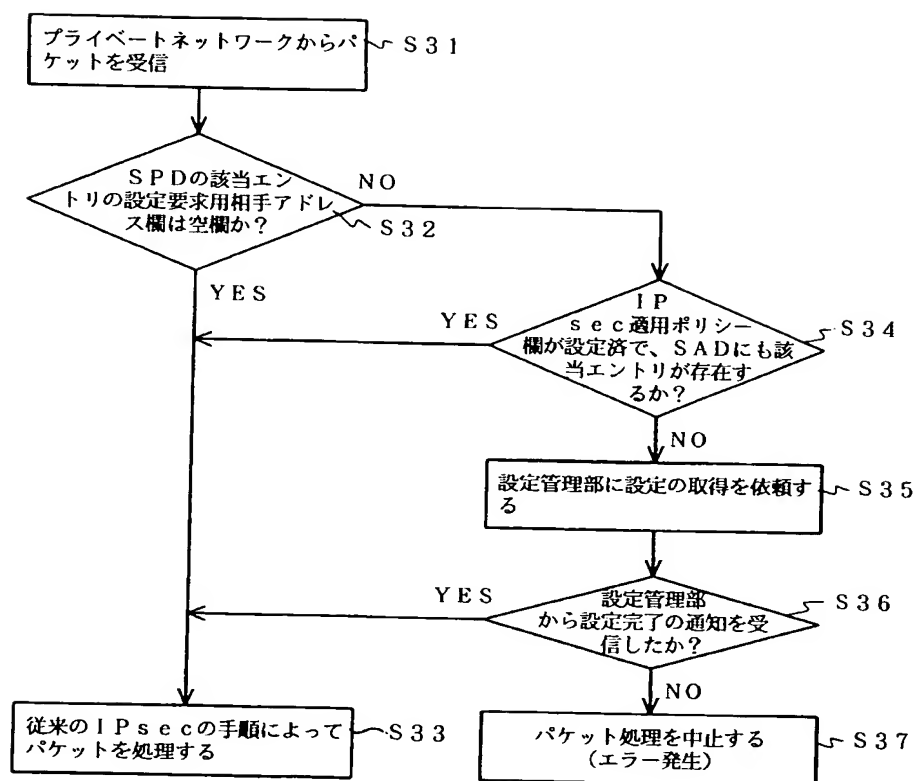
【図 16】

IPsec適用ポリシー	
IPsecプロトコル	ESP
カプセル化モード	トランスポートモード
相手先アドレス	設定サーバ1
暗号化アルゴリズム	AES-CBC
認証アルゴリズム	HMAC-SHA-1-96
SAの有効期間	3600秒
IKEポリシー	
相手IPsec処理装置アドレス	設定サーバ1
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	password-for-ike
暗号化アルゴリズム	DES-CBC
ハッシュアルゴリズム	MD5
Oakleyグループ	1536ビットMODPグループ
SAの有効期間	3600秒

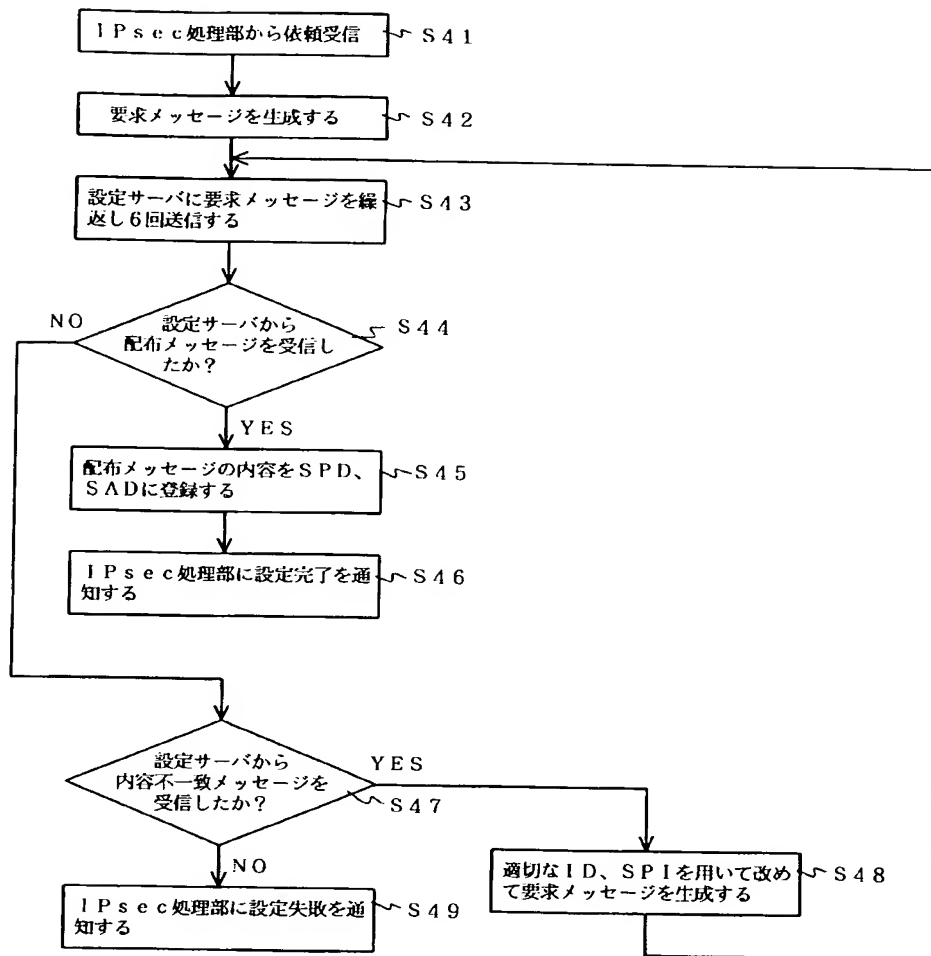
【図17】

ID	キーパラメータ			SAパラメータ
	終点アドレス	IPsec	SPI	
1	IPsec処理装置2b	ESP	6100	カプセル化モード トネルモード 暗号化アルゴリズム DES-CBC 認証アルゴリズム HMAC-MD5-96 暗号化鍵 0x7d5e837ad... 認証鍵 0x83e562bfc... IV 0xc32fbe004... 有効期限 3600秒 シーケンス番号 0
2	設定サーバ1	ESP	6100	カプセル化モード トランスポートモード 暗号化アルゴリズム AES-CBC 認証アルゴリズム HMAC-SHA-1-96 暗号化鍵 0xda738e5d7... 認証鍵 0xcfb265c98... IV 0xc399ebf22... 有効期限 3600秒 シーケンス番号 2133
3				

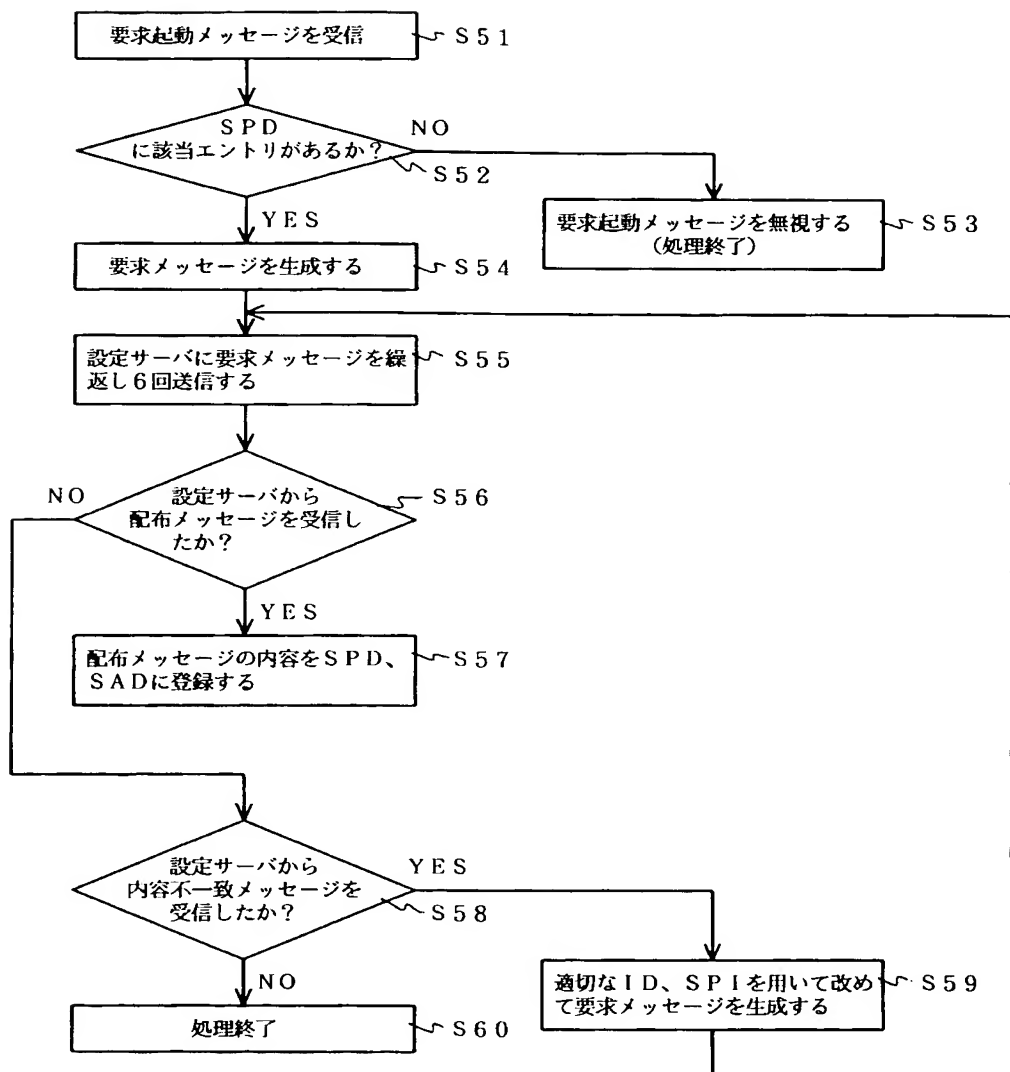
【図 18】



【図 19】



【図 20】



【図 21】

ID	セクタ	処理	IPsec適用ポリシー
1	IPsec設定サーバ1→IPsec処理装置2a	IPsec	適用ポリシー (v)
2	IPsec設定サーバ1→IPsec処理装置2b	IPsec	適用ポリシー (w)
3	IPsec設定サーバ1→IPsec処理装置2c	IPsec	適用ポリシー (x)
4	IPsec設定サーバ1→IPsec処理装置2d	IPsec	適用ポリシー (y)
5	上記以外すべて	廃棄	

【図 22】

IPsec適用ポリシー	
IPsecプロトコル	ESP
カプセル化モード	トランスポートモード
相手先アドレス	IPsec処理装置2a
暗号化アルゴリズム	AES-CBC
認証アルゴリズム	HMAC-SHA-1-96
SAの有効期間	3600秒
IKEポリシー	
相手IPsec処理装置アドレス	IPsec処理装置2a
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	password-for-ike
暗号化アルゴリズム	DES-CBC
ハッシュアルゴリズム	MD5
Oakleyグループ	1536ビットMODPグループ
SAの有効期間	3600秒

【図 23】

I D	セレクト	処理	I P s e c 適用ポリシー
1	プライベート 202宛	I P s e c	適用ポリシー (j)
2	プライベート 203宛	I P s e c	適用ポリシー (k)
3	上記以外すべて	通過	

【図 24】

I P s e c 適用ポリシー	
I P s e c プロトコル	E S P
カプセル化モード	トンネルモード
相手先アドレス	I P s e c 処理装置 2 b
暗号化アルゴリズム	D E S - C B C
認証アルゴリズム	H M A C - M D 5 - 9 6
S A の有効期間	3 6 0 0 秒
I K E ポリシー	
相手 I P s e c 処理装置アドレス	I P s e c 処理装置 2 b
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	p a s s w o r d
暗号化アルゴリズム	D E S - C B C
ハッシュアルゴリズム	M D 5
O a k l e y グループ	1 5 3 6 ビット M O D P グループ
S A の有効期間	3 6 0 0 秒

【図 2 5】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置 2 a	IPsec 処理装置 2 b	1001	5100	適用ポリシー 2 a → 2 b 用 SA パラメータ 2 b → 2 a 用 SA パラメータ 配布ポリシー (a)
	IPsec 処理装置 2 b	IPsec 処理装置 2 a			
2					適用ポリシー
3					

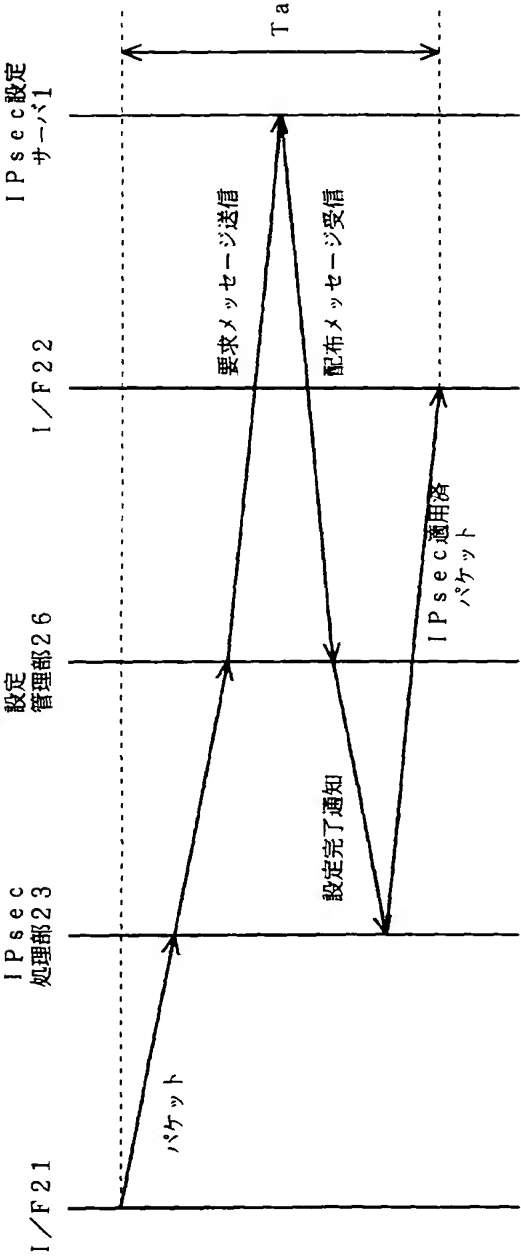
【図 2 6】

I D	セクタ	処理	I P s e c 適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ 1	I P s e c	適用ポリシー (z)	
2	プライベート 2 0 2 宛	I P s e c	適用ポリシー (a)	I P s e c 処理装置 2 b
3	プライベート 2 0 3 宛	I P s e c		I P s e c 処理装置 2 c
4	上記以外すべて	通過		

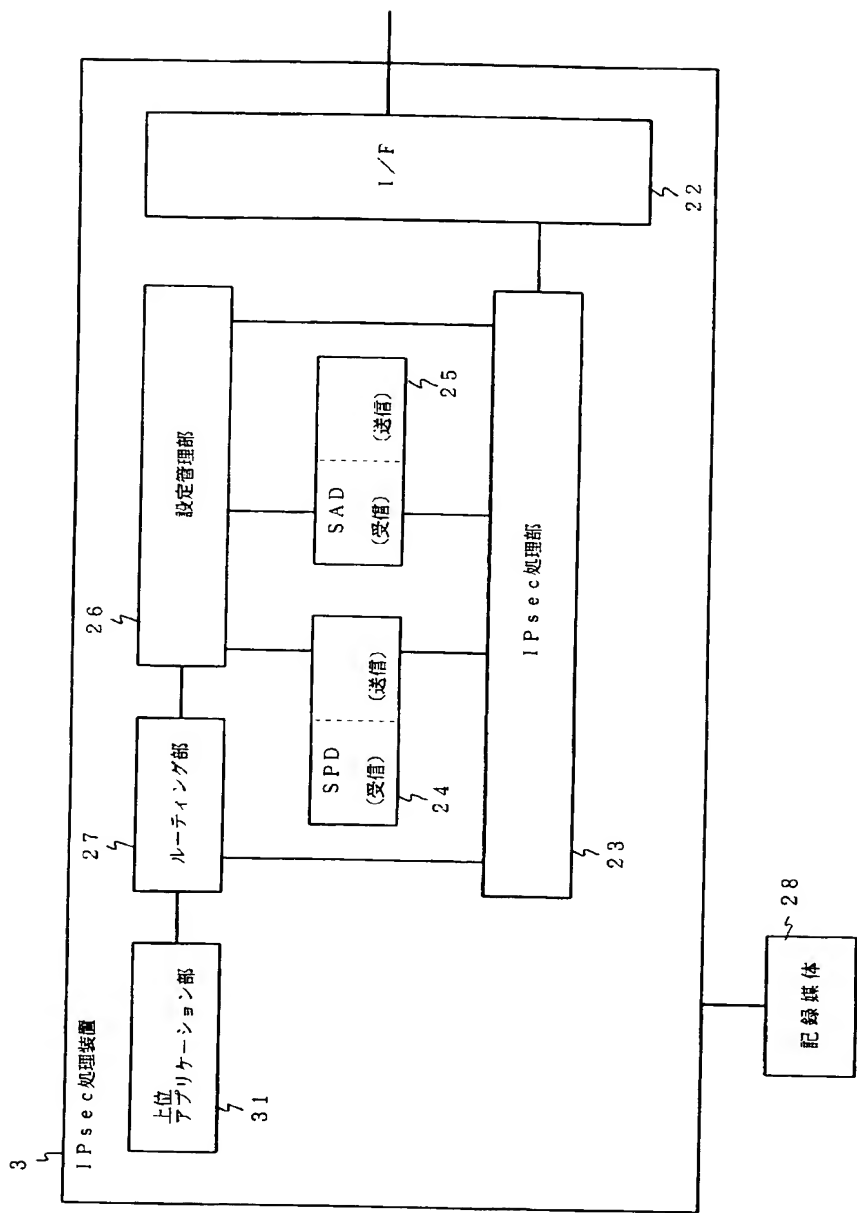
【図 27】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ	
1	IPsec 処理装置2a	IPsec 処理装置2b	1001	5100	適用ポリシー 2a→2b用SAパラメータ	配布ポリシー (a) SAパラメータ (a)
	IPsec 処理装置2b	IPsec 処理装置2a	2001	6100	2b→2a用SAパラメータ	SAパラメータ (b)
2	IPsec 処理装置2a	IPsec 処理装置2b	1002	5110	適用ポリシー 2a→2b用SAパラメータ	配布ポリシー (a) SAパラメータ (c)
	IPsec 処理装置2b	IPsec 処理装置2a	2002	6110	2b→2a用SAパラメータ	SAパラメータ (d)
3						

【図 2 8】



【図 29】



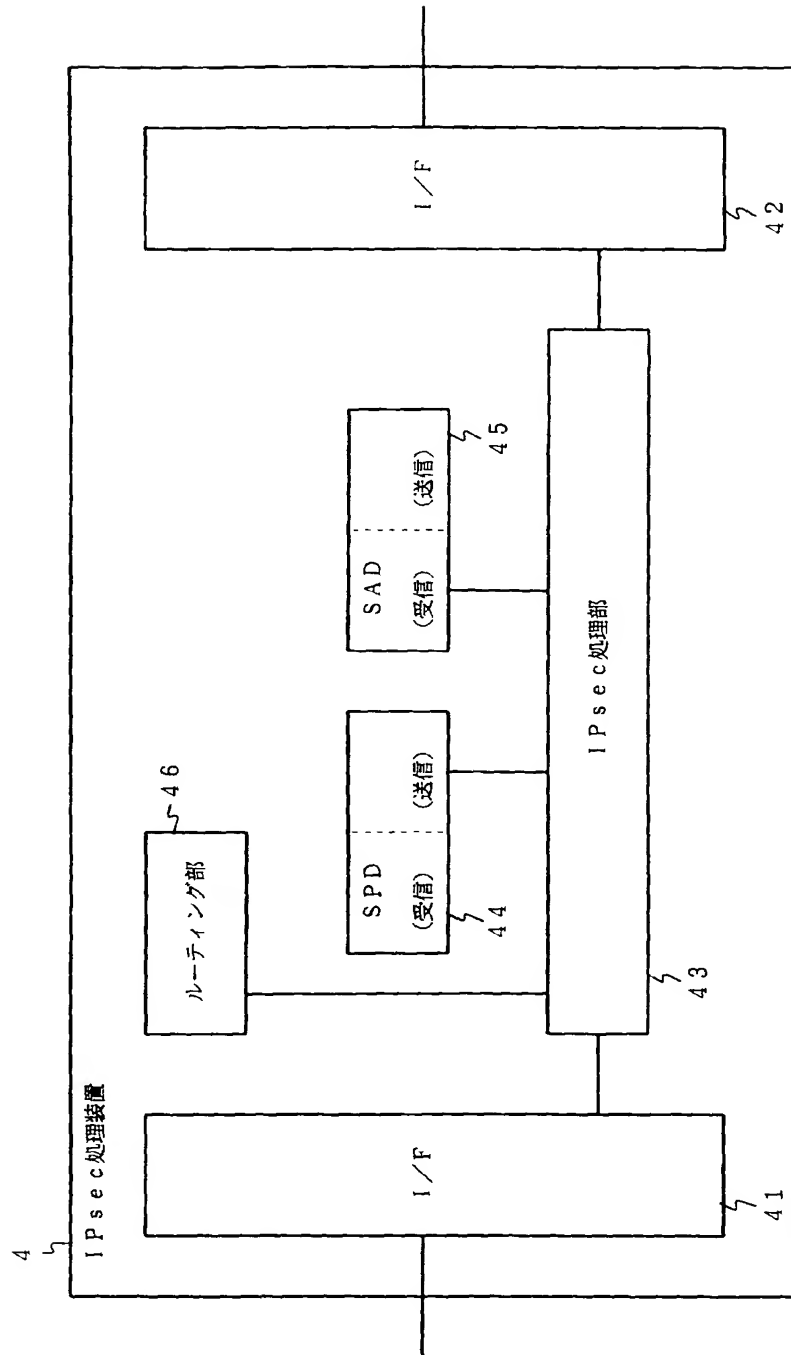
【図 30】

アドレスペア		配布ポリシー
IPsec処理装置2d	IPsec処理装置2e	IPsecプロトコル カプセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間 ESP トランスポートモード 3DES-CBC HMAC-SHA-1-96 3600秒
	上記以外すべて	IPsecプロトコル カプセル化モード 暗号化アルゴリズム 認証アルゴリズム SAの有効期間 ESP トンネルモード DES-CBC HMAC-MD5-96 3600秒

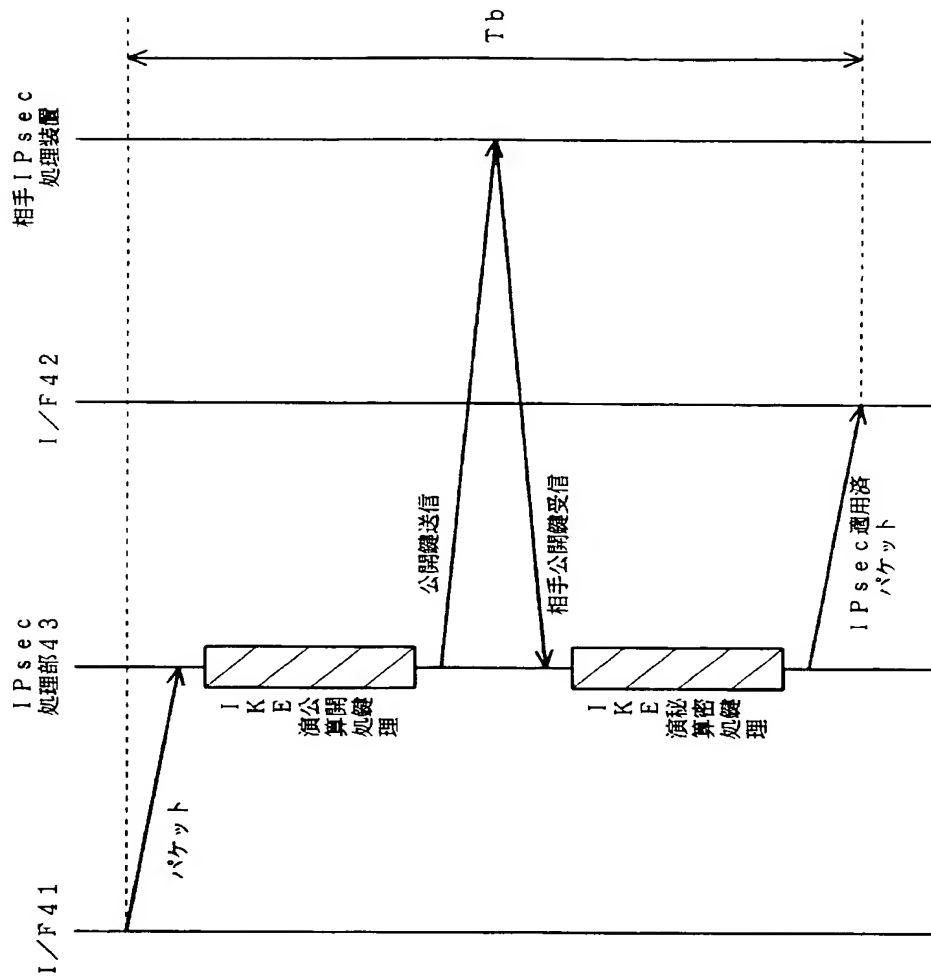
配布ポリシー (b)

配布ポリシー (a)

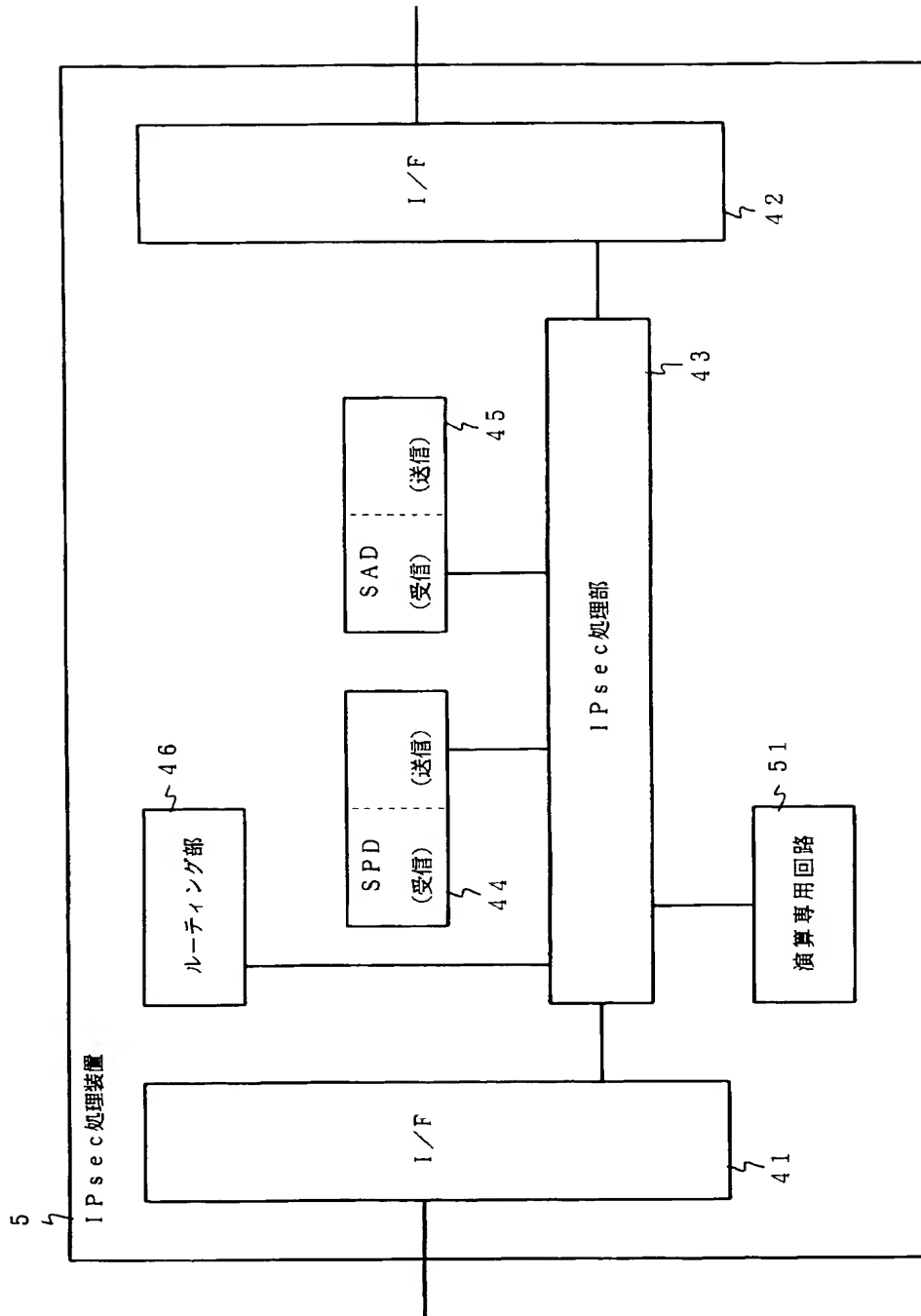
【図 31】



【図 32】



【図 33】



【書類名】 要約書

【要約】

【課題】 通信する装置間での設定不一致を防止可能な I P s e c 設定サーバ装置を提供する。

【解決手段】 I P s e c 処理部 1 2 はインタフェース部 1 1 から受信したデータ通信パケットに対して I P s e c 処理を実施する。S P D 1 3 は I P s e c 処理部 1 2 から参照され、I P s e c を適用するためのポリシーを記録している。S A D 1 4 は I P s e c 処理部 1 2 から参照され、個々の通信に対して I P s e c 処理を実施するために必要な S A を記録している。要求処理部 1 5 は I P s e c 処理装置から設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部 1 6 は要求された設定を決定するために必要な I P s e c ポリシーが記憶されている。管理テーブル 1 7 は設定要求を受けた各々の S A 通信に関する情報が記憶されている。

【選択図】 図 2

特願 2 0 0 2 - 2 6 4 9 1 3

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1 . 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社